DOCUMENT RESUME

ED 176 962 SE 028 639

AUTHOR	Mewborn, Ancel C.; Hively, Wells II
TITLE	A Programmed Course in Algebra.
INSTITUTION	Minnesota Academy of Science, Minneapolis.
SPONS AGENCY	National Science Foundation, Washington, D.C.
PUB DATE	69
NOTE	649p.
EDRS PRICE	MF03/PC26 Plus Postage.
DESCRIPTORS	*Algebra; *College Mathematics; Higher Education; *Mathematics Curriculum; *Mathematics Instruction; *Mathematics Materials; *Number Systems; Secondary Education; Set Theory
IDENTIFIERS	*Functions (Mathematics)

ABSTRACT

This programed textbook consists of short sections of text interspersed with questions designed to aid the student in understanding the material. The course is designed to increase the student's understanding of some of the basic ideas of algebra. Some general experience and manipulative skill with respect to high school algebra is assumed. Emphasis is placed upon development of the logical structure of algebra. Chapter topics include: (1) sets, relations, and functions; (2) algebra of real numbers; (3) algebraic systems; (4) order in the real number system; (5) equations and inequalities; (6) absolute value; (7) completeness of the real number system; (8) natural numbers; (9) integers; (10) rational numbers; (11) complex numbers; (12) algebra of real functions; (13) polynomials; and (14) equivalence relations and groups. (MP)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED176962

A PROGRAMMED COURSE IN ALGEBRA

by ANCEL C. MEWBORN
University of North Carolina

with technical consultation by
WELLS HIVELY II
University of Minnesota

U S DEPARTMENT OF HEALTH,
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY
Mary L. Charles
NSF
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts · Menlo Park, California
London · Don Mills, Ontario

SE 028 639

This book is in the Addison-Wesley Series In Introductory Mathematics

Copyright © 1969 by the Minnesota Academy of Science. All rights reserved.

Printed in U.S.A. and published simultaneously in Canada.

Produced and tested under a grant from the National Science Foundation.

Except for materials covered by copyright of others, permission is hereby granted by the copyright owner and the publisher to all persons to make use of this work after June 30, 1976, provided that publications incorporating materials covered by this copyright contain an acknowledgment of this copyright and a statement that the publication is not endorsed by the copyright holder.

CONTENTS

Foreword iv
Introduction v
Related References vii
How to Use the Program viii
List of Postulates and Theorems x
Unit I Sets, Relations, and Functions 1
Unit II Algebra of Real Numbers 53
Unit III Algebraic Systems 121
Unit IV Order in the Real Number System 176
Unit V Equations and Inequalities 214
Unit VI Absolute Value 263
Unit VII Completeness of the Real Number System 286
Unit VIII Natural Numbers 302
Unit IX Integers 355
Unit X Rational Numbers 386
Unit XI Complex Numbers 416
Unit XII Algebra of Real Functions 459
Unit XIII Polynomials 493
Unit XIV Equivalence Relations and Groups 583

4

FOREWORD

This is a programmed textbook. It is designed to teach. The reader who wishes to survey or review the material it covers, or to look up references, should consult the companion summary textbook; then study unfamiliar material by working on the appropriate sections of this program.

These course materials were produced under a project initiated by Professor Paul C. Rosenbloom. The assistance of the following people in writing and editorial work is gratefully acknowledged: Philip R. Carlson, Bruce P. James, Myra McFadden, Richard S. Presser, Harry L. Patterson, and Sara H. Page. Numerous others contributed to the experimental development of the course: research assistants, volunteer students, and self-sacrificing typists. We thank them all.

A.C.M., W.H.

January, 1969

INTRODUCTION

This course is designed to increase your understanding of some of the basic ideas of algebra. Some general experience and manipulative skill with respect to high school algebra is presumed on your part. Emphasis has been placed upon development of the logical structure. An effort has been made to give a fairly rigorous development of the rules of algebra based upon precise definitions and clearly stated basic assumptions (or postulates).

Special emphasis has been placed upon the real number system. Various mathematical systems which are different from the real number system but which share some of its properties are compared and contrasted with it. In this way the properties of real numbers should be made clearer. For example, there is a definition, often given in algebra textbooks, which says that a negative number is a number which carries a minus sign. This definition is seen to be entirely unsatisfactory when we examine systems in which addition, subtraction, multiplication, and division are defined but in which the notions of "positive" and "negative" have no meaning.

There is, of course, some arbitrariness in our choice of basic assumptions or postulates. In choosing a set of postulates for the real number system or for any other mathematical system one is usually guided by several criteria. First, and most importantly, the postulates should completely describe the system in question. The set of postulates should be complete in the sense that all of the essential properties of the real number system should be derivable from them. No property should be assumed which is not consistent with properties which mathematicians generally regard as being true about the system. Second, some attempt should be made to choose a set of postulates which is few in number. It is not always wise to choose a minimal set of postulates for a system. Attempting to do this might make the task of deriving theorems too difficult. However, there should not be needless duplication. Third, it is often desirable to choose the postulates in such a way that theorems proved for the given system will automatically be known to hold for related systems. For example, the set of postulates which we will give for the real numbers includes a certain set of postulates which are the basic properties for a type of mathematical system called a field. Any theorem which we can prove for the real numbers, and whose proof depends only upon this set of postulates, will automatically be known to hold for any field. The proof does not have to be repeated for other fields.

Even with the use of the above criteria for choosing a set of postulates for a mathematical system, there is still some arbitrariness in the choice. You may find that the set of postulates for the real numbers given in other books differs in certain respects from that which we give here. The important thing to remember is that in developing a mathematical system in a logical way, everything you prove must depend ultimately upon the postulates for the system and the general rules of logic. You cannot be sure that a statement is true about the system unless you can give a proof which depends upon the postulates or upon theorems which have been previously proved from the postulates. Because of this restriction you will find that sometimes you are asked to prove statements which seem obvious. An example of this is the statement "1 is greater than 0". This statement is obvious from your previous experience with real numbers. However, it is not one of the basic assumptions that we make about the real numbers and in our development it requires a proof. Intuition, or the "feel" for what ought to be true, is an invaluable tool for the mathematician. A large part of the training of a student in mathematics should be devoted to the development of his intuition. But along with this he must develop the ability to give logical proofs of propositions which are suggested by his intuition. This is necessary, if for no other reason, because intuition sometimes leads to conclusions which are erroneous.

It is assumed that you are able to recognize certain subsets of the real numbers, although these sets are covered in some detail in the course. The sets in question are listed below.

1. Natural numbers or counting numbers—these are the numbers used in counting—1, 2, 3, 4, . . .
2. Integers—this set is made up of the number 0, the natural numbers, and the additive inverses of the natural numbers—. . . , -3, -2, -1, 0, 1, 2, 3, . . . The positive integers are the natural numbers, the negative integers are the additive inverses of the natural numbers. (We note here that the number 0 is not positive or negative.)
3. Rational numbers—this set consists of all numbers which are quotients, or ratios, of integers. The set of rational numbers contains the set of integers.

RELATED REFERENCES

The following references are strongly recommended; although they are not required for this course, they would be valuable supplements to it. Extensive use of these materials will be of great benefit in increasing your understanding of mathematics, and of algebra in particular.

1. Bell, E. T. *Men of Mathematics.* New York: Simon and Schuster, 1937.
2. Brumfiel, C. F., Eicholz, R. E., and Shanks, M. E. *Algebra II.* Reading, Mass: Addison-Wesley Publishing Co., Inc., 1962. (Ball State Curriculum materials.)
3. Courant, R. and Robbins, H. *What is Mathematics?* New York: Oxford University Press, 1941.
4. Coxeter, H. S. M. *Introduction to Geometry.* New York: John Wiley and Sons, 1961.
5. Haag, V. H. *Studies in Mathematics,* Volume III. *Structure of Elementary Algebra.* New Haven, Conn.: Yale University (SMSG), 1960.
6. Johnson, R. E. *First Course in Abstract Algebra.* Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1953.
7. Keedy, M. L. *A Modern Introduction to Basic Mathematics,* 2nd Ed. Reading, Mass.: Addison-Wesley Publishing Co., Inc., 1969.
8. McCoy, N. H. *Introduction to Modern Algebra.* Boston: Allyn and Bacon, Inc., 1960.
9. Meserve, B. E. and Sobel, M. A. *Mathematics for Secondary School Teachers.* Chapters 1–4, 6–9. Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1962.
10. Polya, G. *How to Solve It.* Garden City, New Jersey: Doubleday and Co., Inc., 1957.
11. Sawyer, W. W. *A Concrete Approach to Abstract Algebra.* San Francisco: W. H. Freeman and Company, 1959.
12. School Mathematics Study Group. *Mathematics for High School, First Course in Algebra.* New Haven, Conn.: Yale University (SMSG), 1960.
13. University of Illinois Committee on School Mathematics. *High School Mathematics.* Urbana, Ill.: University of Illinois Press, 1960.
14. Vance, E. P. *An Introduction to Modern Mathematics,* 2nd Ed. Reading, Mass.: Addison-Wesley Publishing Co., Inc., 1968.

HOW TO USE THE PROGRAM

This course is programmed for "self-instruction". It consists of short sections of text—sometimes just a sentence or two, sometimes several paragraphs—interspersed with questions which are designed to convince both you and the author that you understand what he is trying to say. How well the program works will depend to a large extent on how you use it. When you begin to work you will see a few paragraphs of text followed by a question, a space (or spaces) signalling the need for an answer, and a dotted line:

1. STUDY ONLY THE MATERIAL ABOVE THE DOTTED LINE. USE A PIECE OF CARDBOARD TO COVER UP ALL OF THE PAGE BELOW THE LINE.
2. AFTER YOU HAVE STUDIED THE MATERIAL WRITE AN ANSWER TO THE QUESTION ON A SEPARATE SHEET OF PAPER (A 3 × 5 NOTE PAD IS HANDY).
3. PULL DOWN THE CARDBOARD MASK TO THE NEXT DOTTED LINE. THIS WILL EXPOSE THE AUTHOR'S ANSWER.
4. COMPARE YOUR ANSWER WITH THE ANSWER GIVEN BY THE AUTHOR AND JUDGE WHETHER OR NOT YOUR ANSWER IS CORRECT. YOUR ANSWER MAY NOT BE THE SAME AS HIS IN EVERY DETAIL, BUT IT MAY STILL BE CORRECT. IN ANY CASE, MAKE SURE YOU UNDERSTAND HIS ANSWER.
5. PULL THE MASK DOWN TO THE NEXT DOTTED LINE, STUDY THE TEXT, ANSWER THE NEXT QUESTION, AND SO ON.

It is important to follow these instructions exactly, to use the cardboard mask, and to write out your answer completely using proper notation. Each time you turn a page slip the mask in so that it covers all of the next page before you can see it. Then pull the mask down until you come to the first dotted line. This will keep you from glancing at the answers unintentionally. You may find this routine a bit tedious at first, but it will soon become habitual, and it will pay off in the long run.

Some of the questions may be difficult, and you will have to work hard to answer them. It is important that you force yourself to do so. Do not look at the author's answer until you have made a reasonable attempt to answer the question yourself. This is especially important in proofs of theorems. Before giving up, take time to digest the meaning of the theorem and to find out exactly what the hypothesis is and what is to be proved. Often it will be helpful to review previous material which seems to be related to the theorem.

It is important that you schedule a regular time to work on these materials. You should allow yourself at least an hour at a sitting, and you will probably not want to work much longer than two hours. You can expect the entire course to require about 100 hours of work. Each time you begin work it is wise to review the preceding material in the unit. This is where the summary textbook will come in handy.

To conserve space, postulates and theorems are often referred to by number. The following list should provide a convenient reference to use as you work.

LIST OF POSTULATES AND THEOREMS

II. ALGEBRA OF REAL NUMBERS

POSTULATES

We assume that we have a set R called the real number set upon which are defined two closed binary operations, addition and multiplication, having the following properties:

Names of the Properties	Addition Properties	Multiplication Properties
Associative	A_a: For all a, b, c in R $(a + b) + c = a + (b + c)$.	M_a: For all a, b, c in R $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
Commutative	A_c: For all a, b in R $a + b = b + a$.	M_c: For all a, b in R $a \cdot b = b \cdot a$.
Identity	A_{id}: R contains an element 0 such that $a + 0 = 0 + a = a$ for all a in R.	M_{id}: R contains an element $1 \neq 0$ such that $a \cdot 1 = 1 \cdot a = a$ for all a in R.
Inverse	A_{in}: For each a in R there exists $-a$ in R such that $a + (-a) = -a + a = 0$.	M_{in}: For each a in R, $a \neq 0$, there exists a^{-1} in R such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.
	Addition and Multiplication	
Distributive	D: For all a, b, c in R, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.	

THEOREMS

2.1 If a, b, and x are real numbers and either $a + x = b + x$ or $x + a = x + b$, then $a = b$.

2.2 If a, b, and x are real numbers, with $x \neq 0$, and if either $a \cdot x = b \cdot x$ or $x \cdot a = x \cdot b$, then $a = b$.

2.3 If x is a real number, $x \cdot 0 = 0 \cdot x = 0$.

2.4 If a and b are real numbers and $a \cdot b = 0$, then $a = 0$ or $b = 0$.

2.5 The additive inverse of a real number is unique.

2.6 The multiplicative inverse of a non-zero real number is unique.

2.7 If a and b are real numbers, there is a unique real number d such that $d + a = b$; and furthermore $d = b + (-a)$.

2.8 If a and b are real numbers and $a \neq 0$, there is a unique real number q such that $q \cdot a = b$; and furthermore $q = b \cdot (a^{-1})$.

III. ALGEBRAIC SYSTEMS

THEOREMS

3.1 If a and b are real numbers, $-(a + b) = (-a) + (-b)$.

3.2 If a and b are non-zero real numbers, $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

3.3 $-0 = 0$.

3.4 $1^{-1} = 1$.

3.5 If a is a real number, then $-(-a) = a$.

3.6 If a is a non-zero real number, then $(a^{-1})^{-1} = a$.

3.7 If a and b are real numbers,
  (1) $a \cdot (-b) = -(a \cdot b)$
  (2) $(-a) \cdot b = -(a \cdot b)$
  (3) $(-a) \cdot (-b) = a \cdot b$

3.8 If b is a non-zero real number, $(-b)^{-1} = -(b^{-1})$.

3.9 If a, b, and c are real numbers, then $a \cdot (b - c) = a \cdot b = a \cdot c$.

3.10 If a and b are real numbers and $b \neq 0$, then
  (1) $(-a) \div b = -(a \div b)$
  (2) $a \div (-b) = -(a \div b)$
  (3) $(-a) \div (-b) = a \div b$.

3.11 If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d}.$$

3.12 If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then

$$\frac{a}{b} - \frac{c}{d} = \frac{a \cdot d - c \cdot b}{b \cdot d}.$$

3.13 If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

3.14 If a, b, c, and d are real numbers with $b \neq 0$, $c \neq 0$, and $d \neq 0$, then

$$\frac{a}{b} \div \frac{c}{d} = \frac{a \cdot d}{b \cdot c}.$$

3.15 If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then $\frac{a}{b} = \frac{c}{d}$ if and only if $a \cdot d = c \cdot b$.

3.16 Let G be a group with operation "o" and G' be a group with operation "$\triangle$" and assume that f is an isomorphism of G onto G', then:

- i. If e is the identity of G and $f(e) = e'$, then e' is the identity element of G'.
- ii. The image of the inverse of an element a of G is the inverse of the image of a.

IV. ORDER IN THE REAL NUMBER SYSTEM

POSTULATES

01 Trichotomy (or comparison property): If a and b are real numbers, then one and only one of the following is true: $a < b$, $a = b$, $a > b$.

02 Transitive property: If a, b, c, are real numbers such that $a < b$ and $b < c$, then $a < c$.

03 Addition property: If a, b, c are real numbers such that $a < b$, then $a + c < b + c$.

04 Multiplication property: If a, b, c are real numbers such that $a < b$ and $0 < c$, then $ac < bc$.

THEOREMS

4.1 If a, b, c, d are real numbers such that $a < b$ and $c < d$, then $a + c < b + d$.

4.2 If a, b, c and d are positive real numbers with $a < b$ and $c < d$, then $ac < bd$.

4.3 For real numbers a and b, $a < b$ if and only if $a - b < 0$.

4.4 For real numbers a and b, $a > b$ if and only if $a - b > 0$.

4.5 For any real number b, $b > 0$ if and only if $-b < 0$.

4.6 For any real number b, $b < 0$ if and only if $-b > 0$.

4.7 For real numbers, a and b, $a < b$ if and only if $-b < -a$.

4.8 For real numbers a and b, if $a > 0$ and $b > 0$, then $a + b > 0$.

4.9 For real numbers a and b, if $a < 0$ and $b < 0$, then $a + b < 0$.

4.10 For real numbers a and b, if $a > 0$ and $b > 0$, then $a \cdot b > 0$.

4.11 For real numbers a and b, if $a < 0$ and $b < 0$, then $a \cdot b > 0$.

4.12 For real numbers a and b, if $a > 0$ and $b < 0$, then $a \cdot b < 0$.

4.13 If a is a real number and $a \neq 0$, then $a^2 > 0$.

4.14 For real numbers a, b, c, if $a + c < b + c$ then $a < b$.

4.15 For real numbers a, b, c, if $ac < bc$ and $c > 0$ then $a < b$.

4.16 For real numbers a, b, c, with $c < 0$, $ac < bc$ if and only if $a > b$.

4.17 If a is a real number and if $a > 0$, then $\frac{1}{a} > 0$.

4.18 If a is a real number and if $a < 0$, then $\frac{1}{a} < 0$.

4.19 For real numbers a and b, if $a > b > 0$ then $\frac{1}{b} > \frac{1}{a}$.

4.20 If a, b, c, d are real numbers with $b > 0$ and $d > 0$, then $\frac{a}{b} > \frac{c}{d}$ if and only if $ad > bc$.

4.21 For real numbers a and b if $ab > 0$, then ($a > 0$ and $b > 0$) or ($a < 0$ and $b < 0$).

4.22 For real numbers a and b if $ab < 0$, then ($a > 0$ and $b < 0$) or ($a < 0$ and $b > 0$).

4.23 For real numbers a and b, $ab > 0$ if and only if $\frac{a}{b} > 0$.

4.24 For real numbers a and b, $\frac{a}{b} > 0$ if and only if ($a > 0$ and $b > 0$) or ($a < 0$ and $b < 0$).

4.25 For real numbers a and b, $\frac{a}{b} < 0$ if and only if ($a < 0$ and $b > 0$) or ($a > 0$ and $b < 0$).

4.26 For real numbers a and b, if $a > b > 0$, then $a^2 > b^2$.

4.27 For real numbers a and b, if $a^2 > b^2$, $a > 0$, and $b > 0$, then $a > b$.

VI. ABSOLUTE VALUE

THEOREMS

6.1 If a and b are real numbers, then $|a \cdot b| = |a| \cdot |b|$.

6.2 If a and x are real numbers and $a > 0$, then $|x| < a$ if and only if $-a < x < a$.

6.3 If a and x are real numbers and $a > 0$, then $|x| > a$ if and only if $x > -a$ or $a < x$.

Corollary to Theorem 6.2: If a and x are real numbers and $a > 0$, then $|x| \leq a$ if and only if $-a \leq x \leq a$.

Corollary to Theorem 6.3: If a and x are real numbers and $a > 0$, then $|x| \geq a$ if and only if $x \leq -a$ or $x \geq a$.

6.4 If x and y are real numbers, then $|x + y| \leq |x| + |y|$.

VII. COMPLETENESS OF THE REAL NUMBER SYSTEM

THEOREMS

7.1 If a subset S of R has a least upper bound, then it has only one.

7.2 If a subset S of R has a greatest lower bound, then it has only one.

VIII. NATURAL NUMBERS

POSTULATES

(a) 1 is a natural number.
(b) If n is a natural number, then $n + 1$ is a natural number.
(c) If n is a natural number, then $n \geq 1$.
(d) If n is a natural number, then there is no natural number between n and $n + 1$; i.e., for no natural number m is it true that $n < m$ and $m < n + 1$.

THEOREMS

8.1 If n is a natural number and $n \neq 1$, then $n - 1$ is a natural number.

8.2 The set N of natural numbers is well-ordered.

8.3 (Induction Principle) if S is a subset of N such that
  (a) 1 is in S, and
  (b) if k is any number in S, then $k + 1$ is also in S, then S is all of N.

8.4 The set of natural numbers is closed under addition.

8.5 The set of natural numbers is closed under multiplication.

8.6 If m and q are natural numbers and $m < q$, then $q - m$ is a natural number; i.e., there is a natural number p such that $q = m + p$.

8.7 If n is a natural number and $n = a \cdot b$, where each of a and b is a natural number different from 1, then $1 < a < n$ and $1 < b < n$.

8.8 Every n in N, $n > 1$, is either a prime or has a factorization as a product of primes which is unique except for the order of the factors.

8.9 Let n be a natural number, $n > 1$. If n is not a prime then n has a prime divisor p such that $p^2 \leq n$.

8.10 The set N of natural numbers has no upper bound.

8.11 (Archimedean Property) if a and b are positive real numbers there is a natural number n such that $na > b$.

8.12 If a is a positive real number, there is a natural number n such that $1/n < a$.

IX. INTEGERS

THEOREMS

9.1 If a and b are in I, $b \neq 0$, then there exist q and r in I such that $a = bq + r$ and $0 \leq r < |b|$.

9.2 If b is any integer greater than 1, then any positive integer d may be represented in base b as follows:
$d = c_0 + c_1 b + c_2 b^2 + \cdots + c_n b^n$,
where $c_0, c_1, c_2, \ldots, c_n$ are integers greater than or equal to zero and less than b.

9.3 If $a = bq + r$, $b \neq 0$, then g.c.d. (a, b) = g.c.d. (b, r).

9.4 If d = g.c.d. (a, b), where $a \neq 0$ and $b \neq 0$, then there exist integers k and l such that $d = ka + lb$.

X. RATIONAL NUMBERS

THEOREMS

10.1 There is no rational number $\frac{a}{b}$ such that $\left(\frac{a}{b}\right)^2 = 2$.

XI. COMPLEX NUMBERS

THEOREMS

11.1 If c is a complex number, then $c \cdot \bar{c}$ is a real number. If $c \neq 0$ then $c \cdot \bar{c} > 0$.

11.2 If c is a complex number than $\bar{\bar{c}} = c$. (The conjugate of the conjugate of c is c.)

11.3 If c and d are complex numbers, then $\bar{c} + \bar{d} = \overline{c + d}$.

11.4 If c and d are complex number, then $\bar{c} \cdot \bar{d} = \overline{c \cdot d}$.

11.5 If c is a complex number, then $(\bar{c})^n = \overline{c^n}$, for each natural number n.

11.6 $c \cdot \bar{c} = |c|^2$, for each complex number c.

11.7 If c and d are complex numbers, $d \neq 0$, then $\overline{\left(\frac{c}{d}\right)} = \frac{\bar{c}}{d}$.

11.8 If c and d are complex numbers, then $|c \cdot d| = |c| \cdot |d|$.

11.9 If c and d are complex numbers, $d \neq 0$, then $\left|\frac{c}{d}\right| = \frac{|c|}{|d|}$.

11.10 If c and d are complex numbers, then $|c + d| \leq |c| + |d|$.

XIII. POLYNOMIALS

THEOREMS

13.1 If $P(x)$ and $N(x)$ are polynomials and $N(x) \neq 0$, then there are unique polynomials $Q(x)$ and $R(x)$ such that $P(x) = Q(x) \cdot N(x) + R(x)$ where $R(x)$ is either the zero polynomial or is a non-zero polynomial whose degree is less than the degree of $N(x)$.

13.2 Each non-constant polynomial $P(x)$ has a unique standard factorization of the form $P(x) = c \cdot P_1(x) \cdot P_2(x) \ldots P_k(x)$, where c is a unit and each of $P_1(x), P_2(x), \ldots, P_k(x)$, is an irreducible polynomial whose leading coefficient is one.

13.3 (Remainder Theorem) If $P(x)$ is a (real) polynomial and c is a real number, then the remainder r upon division of $P(x)$ by $x - c$ is a constant polynomial, and $r = P(c)$.

13.4 (Factor Theorem) If $P(x)$ is a non-constant (real) polynomial and c is a real number, then c is a root of $P(x)$ if and only if $x - c$ is a factor of $P(x)$.

13.5 If $P(x)$ is a polynomial of degree $n > 0$, then $P(x)$ has at most n roots.

13.6 If $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, $a_n \neq 0$, $a_0 \neq 0$, and if $\frac{u}{v}$ is a rational root of $P(x)$ written as fraction in lowest terms, then u is a divisor of a_0 and v is a divisor of a_n.

13.7 (Fundamental Theorem of Algebra) If $P(x)$ is a non-constant polynomial with complex number coefficients then there is a complex number c such that $P(c) = 0$; i.e., $P(x)$ has a root in the field of complex numbers.

13.8 If $P(x)$ is a real polynomial and c is a complex number which is a root of $P(x)$, then $\bar{c}$ is also a root of $P(x)$.

13.9 Over the fields of rational numbers, real numbers, and complex numbers, if $P(x)$ and $Q(x)$ are different polynomials then they determine different polynomial functions.

XIV. EQUIVALENCE RELATIONS AND GROUPS

THEOREMS

14.1 If a and b are integers and m is a positive integer greater than 1, then $a \equiv b \pmod{m}$ if and only if $a - b$ is divisible by m.

14.2 If a, b, and c are integers and if m is a positive integer greater than 1, then $a \equiv b \pmod{m}$ if and only if $a + c \equiv b + c$ (mod m).

14.3 If a, b, and c are integers and m is a positive integer greater than 1, and if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.

14.4 If a, b, and c are integers, m is a positive integer greater than 1, and if m and c are relatively prime and $ac \equiv bc \pmod{m}$, the $a \equiv b \pmod{m}$.

14.5 If X is a non-empty set and G is the set of reversible functions from X onto X, then G, together with the operation of composition of functions, is a group.

14.6 If a and b are elements of G such that $a \circ b = b$, then $a = e$.

14.7 If a and b are elements of G and $a \circ b = e$, then $b = a^{-1}$ and $a = b^{-1}$.

14.8 If a, b, and c are elements of G and $a \circ b = a \circ c$, then $b = c$.

14.9 If a and b are elements of G there exists a unique element x of G such that $a \circ x = b$ and a unique element y of G such that $y \circ a = b$.

14.10 If a and b are elements of G, then $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

I. SETS, RELATIONS AND FUNCTIONS

INTRODUCTION

The notion of a "function" is one of the most important in all mathematics. You undoubtedly have some ideas as to what a function is; however the definitions given in high school text books often differ considerably from one book to another. One definition given in many traditional texts is the following: "A variable y is said to be a function of a variable x provided that if a value for x is given then a value for y is determined." Although this definition is inadequate in several respects, it does contain the essential idea of a function; that is, that for any given "value" for x there is paired with it some "value" for y. It is this idea of pairing certain objects with certain other objects which is fundamental in any definition of function. The definition that we will give in this unit is one which brings out most clearly this pairing idea; it is used in many of the newer texts.

Another notion, similar in some respects to that of function, is the notion of a relation. You can think of many situations in mathematics in which there is some kind of relationship between mathematical objects --- (1) less than or greater than for numbers, (2) congruence of polygons in geometry, (3) perpendicularity of lines in geometry, etc. We introduce the concept of "relation" to provide a framework for a systematic study of some of these relationships. The definitions of function and relation which we give have the advantage that a function is a special kind of relation.

In the definitions of function and relation we will use the terms set and ordered pair. We will make no attempt to define these terms, but we will give examples so that you can develop an intuitive feel for what they mean. In mathematics we have to take certain terms as basic and undefined, otherwise we get into circular reasoning. Consider the following list of "dictionary" definitions:

"number - a *collection* of units or individuals."
"collection - a *group* of objects or individuals."
"group - a *number* of persons or things."

Do you think that one can find out what the word number means from the above definitions?

As indicated above we take the terms *set* and *ordered pair* as undefined and define *function* and *relation* in terms of these. To a certain extent, which terms we take as undefined is a matter of choice or taste. We could define *ordered pair* in terms of *set*. This procedure uses fewer undefined terms, but the definition is somewhat artificial. We could take *relation* as undefined and define the other terms in terms of this one.

A definition is neither true nor false. We can, however, justify the choice of a particular definition by showing that the concept we define has the properties we would intuitively expect. Some commonly used texts use definitions of *function* which are *incorrect* in the sense that the concept so defined does not agree with the one everybody uses. Here is an example:

"y is a function of x if to every change in x there is a corresponding change in y."

The function f defined by: $f(x) = 1$, for all x, is not a function according to this definition.

In the first part of this unit sets are discussed. We will not give a detailed exposition of the theory of sets but will simply introduce some notation and terminology which will prove useful later.

SETS

In mathematics the word *set* is used to refer to a collection or aggregate of objects. Thus the words set, collection, and aggregate are synonyms. The objects themselves may be of any nature either physical or conceptual. For example, we speak of the set of letters in the alphabet, the set of states in the United States, the set of points on a line (in geometry), the set of real numbers, the set of solutions (or solution set) of an algebraic equation, etc. The objects or things which make up the collection or set are called elements of the set. Thus we say that k is an element of the set of letters in the alphabet, 5 is an element of the set of real numbers, etc.

List the elements of the set of positive integers less than 6.

- -

ANSWER:

1, 2, 3, 4, 5.

- -

Sets may be described in various ways. One way is to list the members of the set. Thus we will use the notation $\{1, 3, 5, 7\}$ to represent the set whose elements are the numbers 1, 3, 5, 7; i.e., we enclose the listed elements in braces. The order in which the elements are listed is unimportant; $\{1, 3, 5, 7\}$ and $\{3, 7, 1, 5\}$ are the same set.

Using this notation the set of letters used in writing the word number would be denoted by ____.

- -

ANSWER:

$\{b, e, m, n, r, u\}$, or $\{n, u, m, b, e, r\}$, etc. [The order in which the members are listed is not important.]

- -

When listing the elements of a set we never list an element more than once. Thus the set of digits used in writing the number 30253 would be denoted by ____.

- -

ANSWER:

{3, 0, 2, 5}, or {0, 2, 3, 5}, etc. The digit 3 is listed only once.

- -

We can also describe a set by giving a distinguishing property of the elements of the set. Thus the set {1, 3, 5, 7} may be described as "the set of odd whole numbers between 0 and 8." The distinguishing property is that of "being an odd whole number between 0 and 8." The set consists of precisely those objects which have this property.

Why is it not correct to describe the set {1, 4, 9, 16, 25} as "the set of integers which are perfect squares"? (By a "perfect square" we mean the square of an integer.)

- -

ANSWER:

The property given is that "of being an integer which is a perfect square" and there are other numbers which have this property but are not in the given set --- e.g., 36, 49, etc.

- -

To describe a set by a distinguishing property we must choose a property which is possessed by every member of the set and by no element not in the set.

Describe the set {3, 6, 9, 12} by giving a distinguishing property of the set.

- -

ANSWER:

The set of positive integers less than or equal to 12 which are multiples of 3. There may be other correct answers.

- -

We will often use a single capital letter to represent a set. For example we might write:

$A = \{2, 4, 6, 8, 10\}$

and

$B =$ the set of positive even integers less than or equal to 10.

Here A represents a set and B represents a set. Is the set A the same as the set B?

- -

ANSWER:

Yes.

- -

If A and B are sets we say that "A is a subset of B" if every element of A is also an element of B. Symbolically we write "$A \subset B$" or "$B \supset A$" for "A is a subset of B". In this treatment we will consider every set to be a subset of itself; i.e., A A for every set A.

Which of the following statements are true?

(1) The set of integers is a subset of the set of rational numbers.

(2) $\{2, 5, 8, 9\} \supset \{2, 5, 8\}$.

(3) $\{-1, 2, 3\} \subset$ the set of positive integers.

(4) $\{n, b, a, k\} \supset$ the set of letters in the word "bank".

- -

ANSWER:

(1), (2), and (4). (In (3), -1 is not a positive integer.)

- -

Is $\{2, 9\}$ a subset of the set $\{2, 5, 9, 11\}$? ____. Is $\{9, 2\}$ a subset of the set $\{2, 5, 9, 11\}$? ____. Are $\{2, 9\}$ and $\{9, 2\}$ different sets? ____.

- -

ANSWER:

Yes.

Yes.

No.

- -

List all the subsets of the set {2, 5, 9, 11} which have exactly two elements.

- -

ANSWER:

{2, 5}, {2, 9}, {2, 11}, {5, 9}, {5, 11}, {9, 11}.

- -

If a set A is a subset of a set B and B is also a subset of A, what can you say about A and B?

- -

ANSWER:

A and B are the same set.

- -

ORDERED PAIRS AND CARTESIAN PRODUCTS

Recall that in graphing on a coordinate plane with rectangular coordinates it is customary to associate with each ordered pair (x, y) of real numbers x and y a point in the plane. The numbers x and y are called coordinates of the point or members of the ordered pair.

Is the ordered pair (3, 5) associated with the same point as the ordered pair (5, 3)?

- -

ANSWER:

No.

- -

We speak of "ordered" pair because it is necessary to distinguish between pairs with the same members when the members occur in different orders. Thus (3, 5) and (5, 3) are regarded as different ordered pairs

The first member of the ordered pair (5, 3) is the number ____ and the second member is the number ____.

- -

ANSWER:

5, 3

- -

Which one of the order pairs (1, 2), (2, 4), (3, 2), (4, 3) has its first member from the set {1, 2, 3} and its second member from the set {3, 4}?

- -

ANSWER:

(2, 4)

- -

The first and second members of an ordered pair may be the same, as for example in the ordered pair (3, 3).

List all the two-element sets that can be formed with one element from the set {1, 2, 3} and one element from the set {3, 4}. (Be careful.)

- -

ANSWER:

{1, 3}, {1, 4}, {2, 3}, {2, 4}, {3, 4}. Note that {3, 3} is not included since it has only one element, 3. The notation {3, 3} is a violation of our agreement not to list an element of a set more than once.

- -

It will save you some confusion if you will try to use consistently the notation that we have adopted. Always enclose the listed elements of a set in braces while using parentheses to enclose the members of an ordered pair. You should thus write "the set {2, 4}" but "the ordered pair (2, 4)". The choice of this notation is of course arbitrary but consistent use of it will help to prevent your confusing "set" with "ordered pair".

List all the ordered pairs that can be formed with first members from the set {1, 2, 3} and with second members from the set {3, 4}.

- -

ANSWER:

(1, 3), (1, 4), (2, 3), (2, 4), (3, 3), (3, 4).

- -

The ordered pairs in the discussion above have members which are numbers. More generally, we can speak of ordered pairs whose members are objects of any kind. We will see examples of ordered pairs whose members are not numbers a little later.

In mathematics we are often concerned with sets of ordered pairs; i.e., sets whose elements are ordered pairs. Consider the set {(1, 2), (3, 5), (-4, 2)}. The elements of this set are ordered pairs. Is the number 3 an element of the set?

- -

ANSWER:

No (3 is not an ordered pair). The ordered pair (3, 5) is an element of the set.

- -

How many elements are in the set of ordered pairs {(1, 2), (2, 4), (3, 2), (4, 3)}?

- -

ANSWER:

Four; the elements are ordered pairs and there are four ordered pairs.

- -

DEFINITION 1.1: Assume that each of X and Y is a set; X and Y may be the same set or different sets. The Cartesian product of X and Y is the set of all ordered pairs (x, y) such that x is an element of X and y is an element of Y. We denote the Cartesian product of X and Y by X × Y (read "X cross Y").

The Cartesian product X × Y of sets X and Y should not be confused with the ordinary product of multiplication of numbers.

Let X = {1, 2, 3} and Y = {2, 3, 5}.
X × Y is a set and each element of X × Y is a(n) ____.

- -

ANSWER:
ordered pair.

- -

X = {1, 2, 3} Y = {2, 3, 5}

Which of the following ordered pairs are elements of X × Y? (2, 1), (3, 1), (3, 3), (2, 5), (5, 2).

- -

ANSWER:
(3, 3) and (2, 5).

- -

X = {1, 2, 3} Y = {2, 3, 5}
(1) List all the members of X × Y.
(2) List all the members of Y × X.

- -

ANSWER:
(1) (1, 2), (1, 3), (1, 5), (2, 2), (2, 3), (2, 5), (3, 2), (3, 3), (3, 5).
(2) (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (5, 1), (5, 2), (5, 3).

- -

If X is a set with two elements and Y is a set with three elements, how many ordered pairs are in the set $X \times Y$? ____, the set $Y \times X$? ____.

- -

ANSWER:

6,

6.

- -

Let $X = \{1, 2, 3, 4\}$. Is the set $\{1, 3, 4\}$ a subset of $X \times X$? Why?

- -

ANSWER:

No, because the elements 1, 3, and 4 are not ordered pairs. $\{1, 3, 4\}$ is a subset of X.

- -

Find sets X and Y such that

$X \times Y = \{(5, 1), (7, 3), (3, 3), (5, 3), (7, 1), (3, 1)\}$.

- -

ANSWER:

$X = \{5, 7, 3\}$, $Y = \{1, 3\}$

- -

If (x, y) is an element of the Cartesian product of the set of integers and the set of rational numbers, then x is a(n) ____ and y is a(n) ____.

- -

ANSWER:

integer;

rational number.

- -

In graphing on a coordinate plane with rectangular coordinates an ordered pair (x, y) which gives the coordinates of a point is an element of the Cartesian product of the set of real numbers and the set ____.

- -

ANSWER:
of real numbers.

- -

RELATIONS

One of the most important ideas in mathematics is that of a correspondence between the elements of a set X and a set Y (where X and Y may be the same set or different sets). We speak of such a correspondence as a relation between the elements of X and Y. Consider the sentence "A is the father of B". This sentence will be true for many ordered pairs (A, B) of people and false for others. "Is the father of" describes a relation between people.

As another example, consider the sentence "x is less than y", where x is in X, y is in Y, and $X = Y =$ the set of all real numbers. The sentence determines a subset of $X \times Y$ which is the set of all ordered pairs (x, y) for which the sentence is true. "Is less than" describes a relation between numbers. Relations involving the comparison of a pair of elements are known as binary relations. The two examples discussed above are examples of binary relations.

Thus far we have been discussing the concept of relation in a general way, without making a formal definition. We now proceed to do this.

DEFINITION 1.2: A (binary) relation R between a set X and a set Y, is a non-empty subset of $X \times Y$. Thus a relation is a set of ordered pairs.
(Note: The term "non-empty" above simply means that the subset contains at least one element.)

If R is a relation between X and Y, we say x is R-related to y and write $x \, R \, y$ if and only if x is in X, y is in Y, and the ordered pair (x, y) is in the subset of $X \times Y$ which is the relation, i.e., (x, y) is in R.

Let $X = \{1, 2, 3, 4\}$, $Y = \{2, 3, 4\}$, and let R be the set of all ordered pairs, (x, y) where x is in X, y is in Y, and $x \geq y$.

Does this define a binary relation between X and Y?

ANSWER:

Yes.

Let $X = \{1, 2, 3, 4\}$, $Y = \{2, 3, 4\}$, and let R be the set of all ordered pairs, (x, y) where x is in X, y is in Y, and $x \geq y$.

List the elements of the set R.

ANSWER:

$R = \{(2, 2), (3, 2), (3, 3), (4, 2), (4, 3), (4, 4)\}$.

Give the subsets of $X \times Y$ which are the relations defined by the following sentences, where x is in X and y is in Y.

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$.

(a) $x < y$.

ANSWER:

(a) $\{(3, 6), (3, 9), (5, 6), (5, 9)\}$.

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$.

(b) $\sqrt{x} > y$.

ANSWER:

(b) $\{(3, 1), (5, 1)\}$

- -

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$.

(c) $x + y = 10$.

- -

ANSWER:

(c) There are no ordered pairs (x, y) in $X \times Y$ such that $x + y = 10$. Therefore no relation exists.

- -

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$.

(d) $x + y < 10$.

- -

ANSWER:

(d) $\{(3, 1), (3, 6), (5, 1)\}$.

- -

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$.

(e) $x^2 = y$.

- -

ANSWER:

(e) $\{(3, 9)\}$.

- -

$X = \{3, 5\}$ and $Y = \{1, 6, 9\}$

(f) x is a factor of $4y$.

- -

ANSWER:

(f) $\{(3, 6), (3, 9)\}$.

- -

The elements x and y in the ordered pair (x, y) are called the first member and the second member, respectively. It may happen that in the ordered pairs that make up a relation between a set X and a set Y, not all the elements of X or of Y will appear. Since we will want to refer to the set of all first members and the set of all second members that actually do appear in the ordered pairs in the relation, it will be convenient to have names for them. Accordingly, we make the following definition.

DEFINITION 1.3: If R is a relation between X and Y, then the set of all first members of ordered pairs in R is called the domain of R and the set of all second members is called the range of R.

Let $X = \{-7, -4, -1, 2, 5\}$, $Y = \{0, 1, 2, 3, 4\}$, and let R be the set of all ordered pairs (x, y) where x is in X, y is in Y, and $x = 3y - 4$.

(a) List the elements of the set R.

(b) List the set of elements which is the domain of R.

(c) List the set of elements which is the range of R.

ANSWER:

(a) $R = \{(-4, 0), (-1, 1), (2, 2), (5, 3)\}$.

(b) $\{-4, -1, 2, 5\}$.

(c) $\{0, 1, 2, 3\}$.

(Remember to enclose the listed elements of a set in braces.)

DEFINITION 1.4: For any binary relation R between X and Y, consisting of a set of ordered pairs (x, y), there is a second relation obtained by reversing the members in each of the ordered pairs of R, and thus obtaining the set of ordered pairs (y, x). This new relation R^{-1} is said to be the inverse of the relation R. The ordered pair (y, x) is in R^{-1} if and only if (x, y) is in R. That is, $yR^{-1}x$ if and only if xRy.

The roles of the domain and range are interchanged for the inverse of a relation so that the domain of R^{-1} is the ____ of R and the ____ of R is the range of R^{-1}.

- -

ANSWER:

range

domain

- -

Let $X = \{3, 7, 11\}$, $Y = \{4, 11\}$, and let R be the set of all ordered pairs (x, y) in $X \times Y$ such that $x < y$. Then R^{-1} would be the set of all ordered pairs (y, x) in $Y \times X$ such that $x < y$.

(a) List the ordered pairs in R.

(b) List the ordered pairs in R^{-1}.

(c) What is the domain of R? ____ of R^{-1}? ____

(d) What is the range of R? ____ of R^{-1}? ____

- -

ANSWER:

(a) $R = \{(3, 4), (3, 11), (7, 11)\}$.

(b) $R^{-1} = \{(4, 3), (11, 3), (11, 7)\}$.

(c) $\{3, 7\}$; $\{4, 11\}$.

(d) $\{4, 11\}$; $\{3, 7\}$.

- -

A relation is often defined by means of an equation or an inequality. The equation or inequality may contain variables, x and y, which refer to sets X and Y of real numbers. The set of ordered pairs (x, y) for which the equation or inequality is a true statement is a subset of $X \times Y$, and is a relation. The relation may be graphed in a coordinate plane, since it is a set of ordered pairs of real numbers.

Suppose $X = \{2, 4, 6\}$, $Y = \{1, 3\}$, and the relation is the set of all ordered pairs (x, y) where x is in X, y is in Y, and $x = 2y$.

(a) List the ordered pairs in the relation.

(b) Draw a graph of the relation.

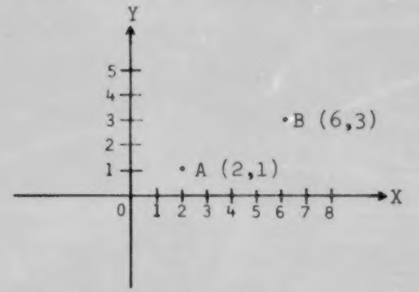
(c) What is the domain of the relation?

(d) What is the range of the relation?

ANSWER:

(a) (2, 1), (6, 3).

(b) The graph consists of just the two points, A(2, 1) and B(6, 3).



(c) The set {2, 6}.

(d) The set {1, 3}.

Suppose X = Y = the set of all real numbers, and the relation *R* is the set of all ordered pairs (x, y) such that $x = 2y - 3$.

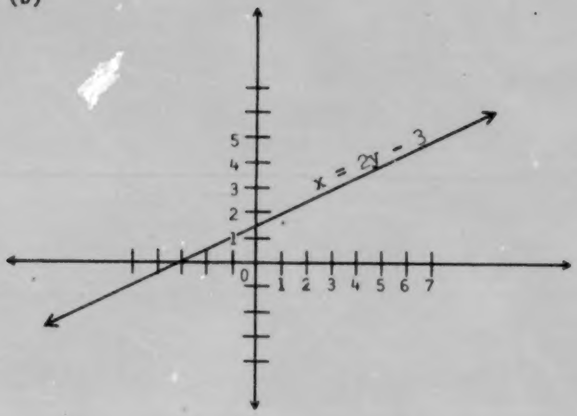
(a) Three ordered pairs in the relation, *R*, are (0, ___), (___, 0), and (5, ___).

(b) Draw the graph of *R*. (Be careful to note that *R* contains all ordered pairs (x, y) such that $x = 2y - 3$.)

ANSWER:

(a) (0, 3/2), (-3, 0), (5, 4).

(b)



- -

Refer to the preceding example. Three ordered pairs in the relation R^{-1} are (1, ___), (___, 5), and (0, ___).

- -

ANSWER:

(1, -1), (4, 5), (0, -3).

- -

To sketch the graph of an equation in x and y it is common procedure to construct a table of values for x and y. For example, if we were interested in sketching the graph of the equation $y = x^3$ near the origin we might construct the following table:

x	y
0	0
1	1
-1	-1
1/2	1/8
-1/2	-1/8
1/4	1/64
-1/4	-1/64

In constructing this table we have actually found seven of the ordered pairs in the relation R consisting of all ordered pairs (x, y) of real numbers such that $y = x^3$. To sketch the graph we plot the points in the x,y-plane determined by the seven ordered pairs $(0, 0)$, $(1, 1)$, $(-1, -1)$, $(1/2, 1/8)$, $(-1/2, -1/8)$, $(1/4, 1/64)$, and $(-1/4, -1/64)$. Then we draw a smooth curve passing through the plotted points. Note that we could not possibly write down all the ordered pairs in the relation R since there are an infinite number of these.

Although in algebra we are primarily concerned with relations involving numbers, the concept of relation permeates all of mathematics and may occur in many different ways. In geometry, for example, we find relations between points, lines, planes, angles, segments, polygons, etc. As an illustration, consider the sentences:

(a) Line ℓ "is parallel to" line m.

(b) Triangle ABC "is congruent to" triangle DEF.

(c) Angle A "is supplementary to" angle B.

Each of the sentences (a), (b), (c), describes a relation. For example; in (a) we are describing the set of all ordered pairs (ℓ, m) such that ℓ and m are lines and $\ell || m$. In (b) we are describing the set of all ordered pairs of triangles, (ABC, DEF), such that Δ-ABC $\cong$ Δ-DEF.

What relation is described in example (c)?

- -

ANSWER:

(c) describes the set of all ordered pairs of angles (A, B) such that A and B are supplementary to each other.

- -

In the preceding examples the words in quotes are the defining words of the relations. The phrase "is vertical to" in geometry describes a relation between a set of angles and ____.

ANSWER:

a set of angles.

- -

Why does the sentence "Angle A is a vertical angle" fail to define a relation?

- -

ANSWER:

It does not give a property of pairs of elements. The notion of vertical angle always involves a pair of angles; so the given sentence is meaningless.

- -

Of the following sentences, some describe relations and some do not. The variables x and y refer to the set of real numbers.

Check the sentences which do not describe relations.

(a) $y^2 = x$

(b) Triangle ABC is isosceles.

(c) Angle A is an alternate interior angle.

(d) Triangle ABC is similar to triangle DEF.

(e) Line m is perpendicular.

(f) Angle A is a right angle.

- -

ANSWER:

(b), (c), (e), (f).

- -

In sentence (a) above, describe the relation completely in terms of ordered pairs.

- -

ANSWER:

The relation is the set of all ordered pairs (x, y) such that x and y are real numbers and $y^2 = x$. (It is also correct to write, "The relation is the set of all ordered pairs (y, x) such that x and y are real numbers and $y^2 = x$." The usual notation for writing ordered pairs involving x and y is to write x as the first member and y as the second. Although we will adopt this convention here, it should be noted that the decision as to which variable is to be written first is entirely arbitrary. Once the variables in the ordered pair have been specified, however, the ordered pairs in the relation must conform to this specification.)

FUNCTIONS

DEFINITION 1.5: A functional relation or function is a relation in which no two ordered pairs have the same first member.

From the definition we see that for no x can we have ordered pairs (x, y_1) and (x, y_2) in a function if $y_1 = y_2$.
Which of the following relations are functions?

(a) the relation $\{(-2, 4), (-1, 1), (0, 0), (1, 1), (2, 4)\}$
(b) the relation $\{(4, -2), (1, -1), (0, 0), (1, 1), (4, 2)\}$
(c) the set of all ordered pairs (x, y) of integers x and y such that $x = 2y$.
(d) the set of all ordered pairs (x, y) of real numbers x and y such that $y^2 = x$.

ANSWER:
(a) and (c). In (b), $(1, -1)$ and $(1, 1)$ are different pairs with the same first member. In (d), these same two pairs occur.

Since a function is a special kind of relation, the notions of domain and range are already defined for functions. What are the domain and range of the function given in part (c) of the previous question?

ANSWER:

domain: the set of even integers.

range: the set of integers.

(It should be noted that the function in part (c) is defined over the integers, and not the real numbers. The defining sentence $x = 2y$ guarantees that for any choice of integer for the second coordinate y in the ordered pair (x, y) the first coordinate x will be 2 times an integer, and hence an even integer.)

- -

Is the following relation a function?

The set of all ordered pairs (x, y) of integers x and y such that $y = 2x + 1$?

- -

ANSWER:

Yes

- -

What are the domain and range of the above function?

- -

ANSWER:

domain: the set of integers.

range: the set of odd integers.

- -

We can completely describe a function by specifying its domain and a rule of correspondence which pairs with each element of the domain some unique element. The function so described consists of all ordered pairs (x, y) such that x is in the domain and y is the element paired with x by the rule.

Consider the function described as follows: the domain of the function is the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ and the rule is -- pair up with each element of the domain the number of its positive integral divisors. For example, the ordered pair (6, 4) is in the function because the number 6 has 4 positive integral divisors, viz. 1, 2, 3, and 6. List all the ordered pairs in the function.

- -

ANSWER:

(1, 1), (2, 2), (3, 2), (4, 3), (5, 2), (6, 4), (7, 2), (8, 4).

- -

Describe the function {(2, 4), (4, 16), (6, 36), (8, 64)} by giving its domain and a rule of correspondence.

- -

ANSWER:

Domain: {2, 4, 6, 8}, Rule: pair up with each element of the domain its square.

- -

We have discussed previously the idea of constructing graphs of relations whose elements are ordered pairs of numbers. We can often tell immediately from the graph of such a relation whether that relation is a function.

What property will the graphs of functions have to distinguish them from the graphs of relations which are not functions? (We assume that the ordered pairs (x, y) in the relation are graphed in the usual way on a rectangular coordinate plane.)

- -

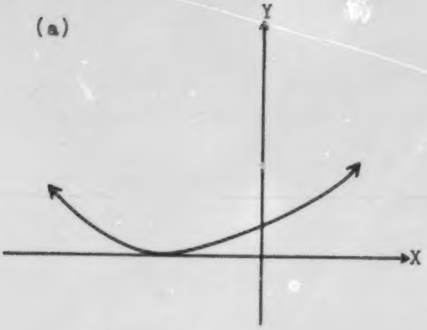
ANSWER:

No vertical line will contain two or more points of the graph.

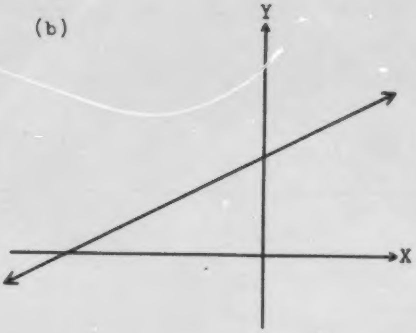
- -

Which of the following are graphs of functions?

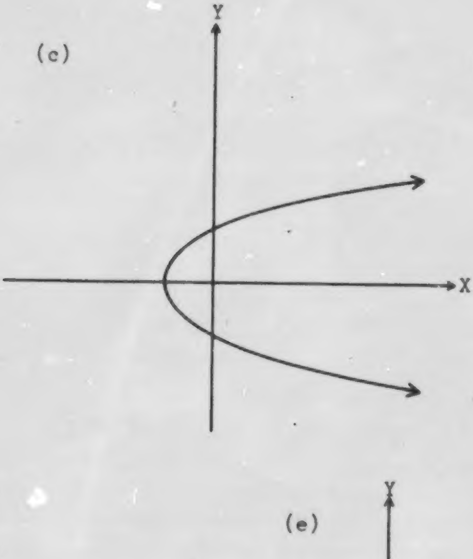
(a)



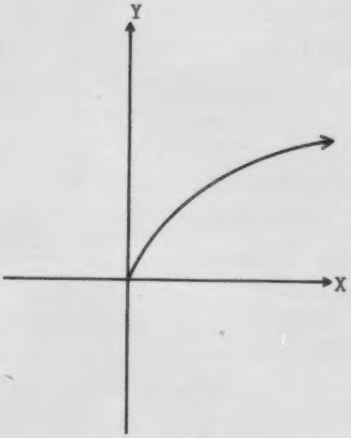
(b)



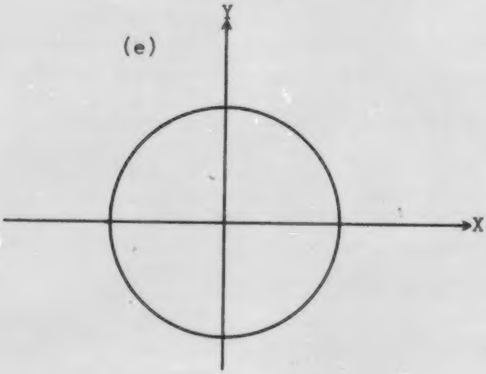
(c)



(d)



(e)



ANSWER:

(a), (b), and (d).

In examples (c) and (e) the y-axis contains two points of the graph. Thus each of these relations contains two ordered pairs with first member 0.

- -

FUNCTIONAL NOTATION

If f denotes a certain function and if x is an element of the domain of f, then f(x) (read "f of x") is used to denote the element of the range of f which is paired with x. Thus, if the ordered pair (3, 18) is in the function f, we would have f(3) = ____.

- -

ANSWER:

f(3) = 18.

- -

The reader is warned against interpreting f(x) as the product of f with x. As stated above, the symbol "f(x)" is simply a convenient notational symbol used to denote the element of the range of f which is paired with x. Thus if x is an element of the domain of f, the ordered pair (x, f(x)) would denote an ordered pair in f.

What difficulty would we encounter if we tried to use the notation f(x) for a relation f which was not a function?

- -

ANSWER:

f(x) would not be uniquely defined for some x. For at least one x in the domain there would be two or more ordered pairs with x as first member.

- -

The above notation is very helpful in giving a rule of correspondence which describes a function.

Let f be the function described by:

$f(x) = x^2 + 2$, for all real numbers x.

The domain of f is the set of all real numbers and the rule of correspondence is: for each x in the domain, pair with x the number ____.

- -

ANSWER:

$x^2 + 2$.

- -

The equation $f(x) = x^2 + 2$ is often incorrectly referred to as a function. The equation is not a function but gives a ____ which, together with specification of the domain, completely describes a function.

- -

ANSWER:

rule of correspondence

- -

The equation $y = x^2 + 2$ defines the above function f. f consists of all ordered pairs (x, y) of real numbers x and y such that the equation holds. Note that in the ordered pair (x, y), x denotes a number in the domain of f and y denotes a number in the range of f. However, be careful to note that it is not correct to say that x is the domain and y is the range. x is used to denote a number in the domain.

You may have a strong tendency to say that "f(x) is a function". This is incorrect. You should say "f is a function". f(x) denotes the element in the range of f which is paired with x by the function f.

Let g be the function defined by:

$g(x) = 1/x$, for all non-zero real numbers x.

What is the domain of g?

- -

ANSWER:

The set of non-zero real numbers.

- -

What is $g(15)$?

What is $g(1/2)$?

What is $g(\sqrt{2})$?

- -

ANSWER:

$g(15) = 1/15$.

$g(1/2) = 2$.

$g(\sqrt{2}) = 1/\sqrt{2}$

- -

What is $g(3) + 1$?

What is $g(4/3)$?

- -

ANSWER:

$g(3) + 1 = 1/3 + 1 = 4/3$.

$g(4/3) = 3/4$.

- -

What is $g(g(3) + 1)$?

- -

ANSWER:

$g(g(3) + 1) = g(4/3) = 3/4$.

- -

What is $g(g(\sqrt{2}))$?

- -

ANSWER:

$g(g(\sqrt{2})) = g(1/\sqrt{2}) = \sqrt{2}$

- -

Another notation which is sometimes used for functions is described in the following: If f is a function and the ordered pair (x, y) is in f then we indicate this fact by the symbol "$x \xrightarrow{f} y$". This notation emphasizes the idea that f determines a rule of correspondence which associates x with y. We sometimes say that f "maps" x to y and call f a "mapping". We can read "$x \xrightarrow{f} y$" as "f maps x to y".

If f is the function defined by:

$f(x) = x^3$, for each real number x, we could write

$2 \xrightarrow{f}$ ____

$-3 \xrightarrow{f}$ ____

____ $\xrightarrow{f} -1$

- -

ANSWER:

8

-27

-1

- -

We could also describe the function f in the following: $x \xrightarrow{f} x^3$, for each real number x.

Using this notation describe the function f consisting of all ordered pairs $(x, x^3 - 3)$ such that x is a real number.

- -

ANSWER:

$x \xrightarrow{f} x^3 - 3$, for each real number x.

If X and Y are sets and R is a relation, we have called R a relation between X and Y is R is a subset of X × Y; i.e., if the domain of R is a subset of ____ and the range of R is a subset of ____.

ANSWER:

X

Y

If f is a function from X to Y and the range of f *is* all of Y we will sometimes say "f is a function from X *onto* Y".

Let us summarize the terminology. If X and Y are sets, a function *from* X *to* Y has a domain that is ____ and a range that is ____.

ANSWER:

all of X

a subset of Y (may or may not be all of Y).

A function from X *onto* Y has a domain that is ____ and a range that is ____.

ANSWER:

all of X

all of Y.

The function f defined by:

$f(x) = 2x$, for each integer x,

is a function from the set of integers to the set of integers and onto the set of even integers because the range of f is ____.

- -

ANSWER:

the set of even integers.

- -

Every function is a function from its ____ onto its ____.

- -

ANSWER:

domain

range

- -

INVERSE OF A FUNCTION

The inverse of a relation is a relation. Therefore, since a function is a special kind of relation, the inverse of a function is a ____.

- -

ANSWER:

relation.

- -

If f is a function with ordered pair (x, y), then the inverse of f, (f^{-1}), is a relation with ordered pair ____.

- -

ANSWER:

(y, x).

- -

Let f be the function defined by $f(x) = x^2$, for each real number x. Two ordered pairs in f are (2, 4) and (-2, 4). Thus (___, 2) and (___, -2) are ordered pairs in f^{-1}.

- -

ANSWER:

(4, 2) and (4, -2).

- -

What can you conclude from the above example about the inverse of a function?

- -

ANSWER:

It need not be a function.

- -

It is clear from the above discussion that if f is a function consisting of the set of ordered pairs (x, f(x)) for all x in the domain of f, then f^{-1} is a relation consisting of ordered pairs (f(x), x), whose domain is the ____ of f.

- -

ANSWER:

range

- -

Thus the role of x and f(x) are interchanged in the inverse of a function.

DEFINITION 1.6: In a function f, for each element of the domain there is exactly one element of the range paired with it. But an element of the range may be paired with several elements of the domain. If f^{-1} is also a function, then each element of the range of f is paired with exactly one element of the domain. If f is a function and f^{-1} is also a function then we say that f is reversible.

Which of the functions f defined in the following are reversible?

(1) $f(x) = x^2$, for each real number x.

(2) $f(x) = x^2$, for each positive real number x.

(3) $f(x) = 2x$ for each integer x.

(4) f is the function $\{(1, 3), (2, 5), (3, 3), (4, 6)\}$.

- -

ANSWER:

(2) and (3).

- -

If f is a reversible function then f sets up a correspondence between the elements of its domain and the elements of its range such that each element of the domain corresponds to exactly one element of the range and each element of the range corresponds to exactly one element of the domain. Therefore if f is a reversible function from X onto Y we say that f defines a one-to-one correspondence between the elements of X and the elements of Y.

The function in example (3) of the preceding exercise defines a one-to-one correspondence between the elements of what two sets?

- -

ANSWER:

The set of integers and the set of even integers.

- -

If f is a reversible function and x is in the domain of f, then $(x, f(x))$ is in the function f and ____ is in the function f^{-1}.

- -

ANSWER:

$(f(x), x)$

- -

Suppose we consider the function f with domain the set of all real numbers and such that

$f(x) = 3x-4$, for each real number x.

The formula $f(x) = 3x-4$ gives $f(x)$ explicitly in terms of x. We can find a similar formula for f^{-1} by replacing, in the formula $f(x) = 3x-4$, x with $f^{-1}(y)$ and $f(x)$ with y, and then solving for $f^{-1}(y)$. Thus $f(x) = 3x-4$ becomes $y = 3f^{-1}(y)-4$.

Solving, we get

$f^{-1}(y) = \frac{y+4}{3}$, for each real number y.

Since $f^{-1}(5) = \frac{5+4}{3} = 3$, then the ordered pair ____ is in f^{-1} and since $f(3) = 3 \cdot 3 - 4 = 5$, the ordered pair ____ is in f.

- -

ANSWER:

(5, 3)

(3, 5)

- -

If the rule for a function f is $f(x) = \frac{2x+3}{5}$ find the rule for f^{-1}.

- -

ANSWER:

Replacing $f(x)$ with y and x with $f^{-1}(y)$, we obtain

$y = \frac{2f^{-1}(y)+3}{5}$ or $f^{-1}(y) = \frac{5y-3}{2}$

- -

In the example above, compute $f(11) =$ ____; $f^{-1}(5) =$ ____

- -

ANSWER:

5

11

If f is the function whose rule is:

$f(x) = \frac{3x + 4}{2x - 3}$, for each real number $x \neq 3/2$, find the rule for f^{-1}.

ANSWER:

$f^{-1}(y) = \frac{3y + 4}{2y - 3}$, for each y in the domain of f^{-1}.

This can be found by replacing $f(x)$ with y and x with $f^{-1}(y)$ in the rule for f as follows:

$$y = \frac{3f^{-1}(y) + 4}{2f^{-1}(y) - 3}$$

$$2f^{-1}(y) \cdot y - 3 \cdot y = 3f^{-1}(y) + 4$$

$$f^{-1}(y) \quad (2y - 3) = 3y + 4$$

$$f^{-1}(y) = \frac{3y + 4}{2y - 3}$$

The result of the last item is interesting in that the rule for f^{-1} is the same as the rule for f. In general, it can be proved that if f is a function whose rule is $f(x) = \frac{ax + b}{cx - a}$ for each real number $x \neq a/c$, then f^{-1} is a function whose rule is also $f^{-1}(y) = \frac{ay + b}{cy - a}$ for each real number $y \neq a/c$. Therefore, $f = f^{-1}$.

DEFINITION 1.7: If X is a set, a very special function with domain X is the function f defined by: $f(x) = x$, for each x in X. This function is called the identity function on X.

Let f be the identity function on the set of real numbers.

(1) Is f a reversible function?

(2) What is the range of f?

(3) What is $f(\sqrt{3})$?

ANSWER:

(1) Yes.

(2) The set of real numbers.

(3) $f(\sqrt{3}) = \sqrt{3}$.

COMPOSITION OF FUNCTIONS

Let f and g be the functions defined as follows:

$f(x) = 1/x$, for each non-zero real number x.

$g(x) = x^2 - 1$, for each real number x.

(1) What is $f(g(2))$?

(2) What is $g(f(2))$?

(3) Why does $f(g(1))$ have no meaning?

ANSWER:

(1) $f(g(2)) = f(3) = 1/3$.

(2) $g(f(2)) = g(1/2) = -3/4$.

(3) $g(1) = 0$ and 0 is not in the domain of f.

We define the composite of f with g given above to be the function h defined by: $h(x) = f(g(x))$, for each real number x such that $x^2 - 1 \neq 0$. We require that $g(x) \neq 0$ because ____.

ANSWER:

0 is not in the domain of f.

DEFINITION 1.8: In general, if f and g are functions we define the composite of f with g to be the function h such that $h(x) = f(g(x))$, for each x in the domain of g for which $g(x)$

is in the domain of f. Note that g(x) has meaning only if x ____, and f(g(x)) has meaning only if g(x) ____.

- -

ANSWER:

is in the domain of g.

is in the domain of f.

- -

We denote the composite of f with g by f o g.

Let f and g be functions defined as follows:

$f(x) = 2x^2 + 2$, for each real number x,

$g(x) = \sqrt{1 - x}$, for each real number x less than or equal to 1.

What is the range of f?

- -

ANSWER:

The set of real numbers greater than or equal to 2.

- -

Is there a number x in the domain of f such that f(x) is in the domain of g?

- -

ANSWER:

No; for every x in the domain of f, $f(x) \geq 2$, and numbers greater than or equal to 2 are not in the domain of g.

- -

Therefore the composite g o f is not defined in this case. However f o g is defined. What is the domain of f o g?

- -

ANSWER:

The set of real numbers less than or equal to 1.

- -

What is $f \circ g(-3)$?

- -

ANSWER:

$f \circ g(-3) = f(g(-3)) = 10.$

- -

As another example, let f and g be functions defined as follows:

$f(x) = x^2 - 3$, for each real number x,

$g(x) = \sqrt{x + 4}$, for each real number x greater then or equal to -4.

What is the range of f?

- -

ANSWER:

The set of real numbers greater than or equal to -3.

- -

Is there a number x in the domain of f such that $f(x)$ is not in the domain of g?

- -

ANSWER:

No; for every x in the domain of f, $f(x) \geq -3$, and numbers greater than or equal to -3 are in the domain of g.

- -

Is the composite $g \circ f$ defined in this case?

- -

ANSWER:

Yes.

- -

We may find the rule for the composite of $g \circ f$ in the above example as follows:

$(g \circ f)(x) = g(f(x)) = g(x^2 - 3) = \sqrt{(x^2 - 3) + 4} = \sqrt{x^2 + 1}$, for each real number x in the domain of f. Thus if 4 is in the domain of f, we may find $(g \circ f)(4)$ by replacing x with 4 in $\sqrt{x^2 + 1}$ obtaining $\sqrt{17}$. Thus the ordered pair ____ is in the function $g \circ f$.

- -

ANSWER:
$(4, \sqrt{17})$

- -

In the last example, is the composite $f \circ g(x)$ defined for every real number x?

- -

ANSWER:
No; $f \circ g(x)$ is not defined for $x < -4$ since these values of x are not in the domain of g.

- -

What is the domain of $f \circ g$?

- -

ANSWER:
The set of real numbers greater than or equal to -4.

- -

Find the rule for the composite $f \circ g$.

- -

ANSWER:
$(f \circ g)(x) = f(g(x)) = f(\sqrt{x + 4}) = (\sqrt{x + 4})^2 - 3 =$
$x + 4 - 3 = x + 1$, for each real number x in the domain of g.

What is $(f \circ g)(5)$?

ANSWER:

$(f \circ g)(5) = f(g(5)) = f(3) = 6$; or, since $(f \circ g)(x) = x + 1$, $(f \circ g)(5) = 5 + 1 = 6$.

What is $(f \circ g)(-5)$?

ANSWER:

$(f \circ g)(-5)$ is not defined since -5 is not in the domain of g.

What is $(g \circ f)(-5)$?

ANSWER:

$(g \circ f)(-5) = g(f(-5)) = g(22) = \sqrt{26}$; or, since $(g \circ f)(x) = \sqrt{x^2 + 1}$, then $(g \circ f)(-5) = \sqrt{(-5)^2 + 1} = \sqrt{26}$.

What is $(f \circ g)(0)$?

ANSWER:

$(f \circ g)(0) = f(g(0)) = f(2) = 1$; or, since $(f \circ g)(x) = x + 1$, then $(f \circ g)(0) = 0 + 1 = 1$.

The notion of the composite of two functions can be made a little clearer by the following. Suppose f and g are functions. If x is in the domain of g we can write $x \xrightarrow{g} g(x)$. If $g(x)$ is in the domain of f we can write $g(x) \xrightarrow{f}$ ____.

ANSWER:

$f(g(x))$

Thus $x \xrightarrow{g} g(x) \xrightarrow{f} f(g(x))$. Hence we can regard $f \circ g$ as the result of successive "mappings" by the functions ____ and ____, in that order.

ANSWER:

g, f

The following notation is suggestive.

$$\begin{tikzcd} x \arrow[r, "g"] \arrow[rr, bend left, "f \circ g"] & g(x) \arrow[r, "f"] & f(g(x)). \end{tikzcd}$$

Do $(f \circ g)(x)$ and $f(g(x))$ denote the same thing?

ANSWER:

Yes.

If g is the identity function on a set X, then we have

$x \rightarrow$ ____, for every element x in X.

ANSWER:

x.

Let g be the identity function on the set of all real numbers and let

$f(x) = 2x^2 + 1$, for every real number x.

Then

$x \xrightarrow{f}$ ____ $\xrightarrow{g}$ ____, for every real number x,

and

$x \xrightarrow{g}$ ____ $\xrightarrow{f}$ ____, for every real number x.

ANSWER:

$2x^2 + 1$, $2x^2 + 1$

x , $2x^2 + 1$

This shows that

$x \xrightarrow{g \circ f}$ ____, for every real number x,

and

$x \xrightarrow{f \circ g}$ ____, for every real number x.

ANSWER:

$2x^2 + 1$

$2x^2 + 1$

Therefore $g \circ f = f$ and $f \circ g = f$. In a similar way it can be seen that if f is a function from a set X to a set Y and if g is the identity function on X then $f \circ g =$ ____.

ANSWER:

f

Similarly $h \circ f = f$ if h is the identity function on ____.

ANSWER:

Y.

If f is a reversible function, is f^{-1} a reversible function?

ANSWER:

Yes.

Let f be a reversible function with domain X and range Y. Then f^{-1} is a reversible function with domain ____ and range ____.

ANSWER:

Y, X.

If x is in X then $x \xrightarrow{f} f(x) \xrightarrow{f^{-1}}$ ____; i.e., $(f^{-1} \circ f)(x) =$ ____.

ANSWER:

x; x.

Therefore $f^{-1} \circ f$ is the ____ function on X.

ANSWER:

identity

$f \circ f^{-1}$ is the identity function on ____.

ANSWER:

Y.

- -

Let f be a reversible function from a set X onto a set Y. If g is any function from Y to X such that either $f \circ g$ is the identity function on Y or $g \circ f$ is the identity function on X, then g is necessarily f^{-1}.

For example, assume that $f \circ g$ is the identity function on Y. If (y, x) is any ordered pair in g, then $g(y) = x$. Hence $f(x) = f(g(y)) = f \circ g(y) = y$, and so (x, y) is in f. Conversely, if (x, y) is in f, then $y = f(x)$. But $y = f \circ g(y) = f(g(y))$. Hence $(g(y), y)$ is also in f. Since (x, y) and $(g(y), y)$ are ordered pairs in f and f is reversible, $x = g(y)$. Hence (y, x) is in g. Therefore (y, x) is in g if and only if (x, y) is in f. So $g = f^{-1}$

IMPLICITLY DEFINED FUNCTIONS

Although functions arise in many situations in mathematics, they do not usually arise with the precise formulation that we have assumed; i.e., as a set of ordered pairs. For example, we sometimes see such statements as: the volume of a cube is a function of the length of a side. Implicit in this statement is the function consisting of all ordered pairs (s, v) of real numbers such that there is a cube with side of length s and volume v. We know from geometry that $v = s^3$. So the function f involved here may be described by:

$f(s) = s^3$, for each positive real number s.

Describe the function f implicit in the following statement, giving the domain and a rule of correspondence: The area of a circle is a function of its diameter.

- -

ANSWER:

f consists of all ordered pairs (d, a) of real numbers such that there is a circle with diameter d and area a. f may be described by:

$$f(d) = \frac{\pi d^2}{4}, \text{ for each positive real number } d,$$

or

$$f: d \to \frac{\pi d^2}{4}, \text{ for each positive real number } d.$$

Refer to the above function. Criticize the statement: For the function $f(d)$, d is the domain and a is the range.

ANSWER:

The function is denoted by f, not $f(d)$. $f(d)$ denotes the number paired with the number d by the function f. Also d is not the domain and a is not the range; d refers to a number in the domain and a refers to a number in the range.

What is the domain of the above function f?

ANSWER:

the set of positive real numbers.

Suppose the locus of a point P in a plane is such that its distance r from a fixed point A and its distance s from a fixed point B are related by the equation

$$rs = 10$$

We say that s is defined as function of r. Give an explicit description of the function f implicit in the above description.

ANSWER:

The function f is the set of all ordered pairs (r, s) such that r and s are positive numbers and $r \cdot s = 10$. Other ways of describing the function are:

$f(r) = 10/r$, for each positive real number r,

$r \xrightarrow{f} 10/r$, for each positive real number r.

Most of the functions that we have discussed so far have had domains which were sets of real numbers. These functions are often referred to as "functions of one real variable". However, consider the statement: the volume of a cylinder is a function of the radius of the base and of the height. Let us see if we can determine what function is implicit in this statement. If we are given the radius, r, of the base of a cylinder and height, h, then we can determine the volume. Thus for each ordered pair (r, h) of positive real numbers there is a unique positive real number v paired with it. Thus we have determined a function f whose domain is the set of all ordered pairs (r, h) of positive real numbers r and h.

The function f consists of ordered pairs whose first members are ____ and whose second members are ____.

ANSWER:

ordered pairs of positive real numbers

positive real numbers

An ordered pair in f would have the form $((r, h), v)$. A less confusing notation is

$(r, h) \xrightarrow{f} v$.

We know that $v = \pi r^2 h$. So

$f((r, h)) =$ ____.

ANSWER:

$\pi r^2 h$

Usually we do not write both parentheses in $f((r, h))$ but write simply $f(r, h)$.

A function whose domain is a set of ordered pairs of real numbers is often called a "function of two real variables". By analogy a "function of three real variables" would be one whose domain is a set of ____.

ANSWER:

ordered triples of real numbers.

Describe the function f implicit in the following statement, giving the domain and a rule of correspondence: the volume of a rectangular parallelopiped is a function of its length, width, and height.

ANSWER:

The domain of f is the set of ordered triples (ℓ, w, h) where ℓ, w, and h are the length, width, and height of some rectangular parallelopiped. The function may be described by:

$(\ell, w, h) \xrightarrow{f} \ell \cdot w \cdot h$, for each ordered triple (ℓ, w, h) of positive real numbers.

or by:

$f(\ell, w, h) = \ell \cdot w \cdot h$, for each ordered triple (ℓ, w, h) of positive real numbers.

(Have you specified the domain in your answer?)

REVIEW ITEMS

1. Describe the set $\{1, 4, 9, 16, 25\}$ by giving a distinguishing property of the set.

ANSWER:

The set of positive integers equal to or less than 25 which are perfect squares. (Note: There are other correct answers.)

---

2. Which of the following statements are true?

(a) The set of natural numbers is a subset of the set of integers.

(b) $\{t, i, n\} \subset$ the set of letters in the word "integer".

(c) $\{3, 4\}$ and $\{4, 3\}$ are different sets.

ANSWER:

(a) and (b) are true.

---

3. How many subsets of the set $\{a, b, c, d\}$ contain exactly three elements?

ANSWER:

4.

---

4. Is the number 5 an element of the set $A \times B$ if $A = (2, 5)$ and $B = \{3, 5, 7\}$? If not, why?

ANSWER:

No. The elements of $A \times B$ are ordered pairs, and 5 is not an ordered pair.

---

5. List all the elements of $A \times B$ if $A = \{2, 5\}$ and $B = \{3, 5, 7\}$ as in Item 4.

ANSWER:

$\{(2, 3), (2, 5), (2, 7), (5, 3), (5, 5), (5, 7)\}$.

---

6. What must be true about sets A and B if $A \times B = B \times A$?

ANSWER:

They must be the same set; i.e., $A = B$.

---

7. Let $A = \{2, 4, 6\}$, $B = \{1, 3, 5, 7\}$, and R be the set of all ordered pairs (x, y) such that x is in A, y is in B, and $x + y > 10$.

(a) List the elements of R.
(b) List the elements in the domain of R.
(c) List the elements in the range of R.
(d) Describe the set R^{-1} in words.
(e) List the elements in R^{-1}.
(f) List the elements in the domain of R^{-1}.
(g) List the elements in the range of R^{-1}.

ANSWER:

(a) $R = \{(4, 7), (6, 5), (6, 7)\}$.
(b) Domain of $R = \{4, 6\}$.
(c) Range of $R = \{5, 7\}$.
(d) R^{-1} is the set of all ordered pairs (y, x) such that y is in B, x is in A, and $x + y > 10$.
(e) $R^{-1} = \{(7, 4), (7, 6), (5, 6)\}$.
(f) Domain of $R^{-1} = \{5, 7\}$.

(g) Range of $R^{-1} = \{4, 6\}$.

- -

8. Let R be the set of all ordered pairs of real numbers (x, y) such that $3x - 2y = 9$. Describe the graph of R.

- -

ANSWER:

The graph of R is the set of all points on a line (whose equation is $3x - 2y = 9$).

- -

9. Let $S = \{5, 7, 8, 10\}$ and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and $x + y = 15$. Describe the graph of R.

- -

ANSWER:

The graph of R consists of just the four points whose coordinates are $(10, 5)$, $(5, 10)$, $(7, 8)$, $(8, 7)$.

- -

10. Every function is a relation. Is it true that every relation is a function?

- -

ANSWER:

No.

- -

11. Describe the following function completely by giving its domain and a rule of correspondence: $f = \{(1, 4), (3, 12), (5, 20), (7, 28), (9, 36), (11, 44), (13, 52)\}$.

- -

ANSWER:

The domain of f is the set of positive odd integers less than 15. The rule is "pair with each x in the domain of f the element $4 \cdot x$".

---

12. Let f be the function defined by:

$f(x) = 2x - 1$, for each integer x.

(a) What is the domain of f?

(b) What is the range of f?

ANSWER:

(a) The set of integers.

(b) The set of odd integers.

---

13. Let f be a function defined by:

$f(x) = x^2 + 7$, for all real numbers x.

(a) What is the range of f?

(b) Is this a function onto the set of real numbers?

ANSWER:

(a) The range of f is the set of all real numbers ≥ 7.

(b) No.

---

14. The functions f and g are defined as follows:

$f(x) = x^2 - 3$, for each real number x.

$g(x) = \sqrt{2x + 1}$, for each real number $x \geq -1/2$.

(a) What is the range of f?

(b) What is the domain of $f \circ g$?

(c) What is $f(1/2)$?

(d) What is $g(1/2)$?

(e) Find the rule for $(f \circ g)(x)$.

(f) What is $(f \circ g)(-2)$?

- -

ANSWER:

(a) The range of f is the set of all real numbers greater than or equal to -3.

(b) The domain of $f \circ g$ is the set of all real numbers $\geq -1/2$

(c) $f(1/2) = -11/4$

(d) $g(1/2) = \sqrt{2}$

(e) $(f \circ g)(x) = 2x - 2$, for each real number $x \geq -1/2$

(f) (-2) is not in the domain of g nor of $f \circ g$, so $(f \circ g)(-2)$ is not defined.

- -

15. Let f be the function defined by:

$f(x) = 2x + 3$, for all real numbers x.

Find a function g such that $f \circ g$ is the identity function.

- -

ANSWER:

g is the function such that $g(x) = \frac{x-3}{2}$ for all real numbers x. The rule for g can be found as follows:

$$\begin{aligned} \text{Since we want } (f \circ g)(x) &= x \\ \text{then } f(g(x)) &= x \\ \text{or } 2 \cdot g(x) + 3 &= x \\ \therefore g(x) &= \frac{x-3}{2}, \text{ for all real numbers } x. \end{aligned}$$

- -

16. If f is a function, then f^{-1} is a relation. Is it necessarily true that f^{-1} is also a function?

- -

ANSWER:

No.

- -

17. Let f and g be functions defined by:

$f(x) = 3x - 1$, for each real number x.

$g(x) = x^2 - 4$, for each real number x.

(a) Is f^{-1} a function?

(b) Is g^{-1} a function?

(c) Find the rule for f^{-1}.

(d) Compute $(f \circ f^{-1})(5)$.

- -

ANSWER:

(a) Yes

(b) No

(c) $f^{-1}(x) = \frac{x + 1}{3}$, for each real number x.

(d) $(f \circ f^{-1})(5) = 5$.

- -

18. Describe the function f implicit in the following statement, giving the domain and a rule of correspondence: The area of a triangle is a function of its base and height.

- -

ANSWER:

The domain of f is the set of ordered pairs (b, h) where b and h are the base and height of some triangle. The function may be described by $f(b, h) = 1/2b \cdot h$, for each ordered pair (b, h) of positive real numbers.

- -

19. Let $X = Y =$ the set of all real numbers. Let R be the relation between X and Y consisting of all ordered pairs (x, y) in

$X \times Y$ such that $3x > 2y + 1$. Which of the following is (are) correct?

(a) R^{-1} is the set of all ordered pairs (x, y) in $X \times Y$ such that $3x < 2y + 1$.

(b) R^{-1} is the set of all ordered pairs (y, x) in $Y \times X$ such that $3x > 2y + 1$.

(c) R^{-1} is the set of all ordered pairs (y, x) in $Y \times X$ such that $3x < 2y + 1$.

- -

ANSWER:

(b) is correct, (a) and (c) are not correct. (Remember that (y, x) is in R^{-1} if and only if (x, y) is in R).

- -

20. Let f be the function defined by:

$f(x) = 3x^2 + 2$, for all real numbers x.

Is the following a correct way of finding $f(2)$?
Explain.

$f(2) = f(3(2)^2 + 2) = f(12 + 2) = 14.$

- -

ANSWER:

No. The result is correct, $f(2) = 14$. However, the f in the second and third expressions should be omitted. A correct version is:

$f(2) = 3(2)^2 + 2 = 12 + 2 = 14.$

(Note: This kind of error was made by many students in an experimental version of this course.)

- -

II. ALGEBRA OF REAL NUMBERS

INTRODUCTION

The foundation upon which most of the mathematics in high school algebra and elementary calculus courses is based is the real number system. A great deal of the work done in high school algebra is designed to give the student basic manipulative skills in working with real numbers. The student is given a set of rules, or principles, by which he learns to solve equations, factor algebraic expressions, etc. These skills are important, and the student will not go very far in mathematics without them. But students need to gain more than this from their study of mathematics. Another goal of the teacher of mathematics should be to help students learn something about logical reasoning and precision of thought. It is traditional to teach the geometry course in the high school in a way that emphasizes the logical structure of geometry, but this approach has been notably absent from courses in algebra. Everyone knows that one proves theorems in geometry but it often comes as a surprise, even to teachers of mathematics, that the same can be true of algebra. The algebra of the real numbers is just as well suited to study as a logical system as is plane geometry.

In this unit many of the usual rules and principles for working with real numbers will be presented. However, these will be given in a way that emphasizes the logical dependency of some of these rules upon others. We will choose a few of these rules or properties as basic assumptions or postulates. We will then derive the other properties as theorems. Proofs of most of these theorems will be required. At first the proofs will be outlined for you and you will only have to supply a few missing steps or reasons. Later you will be asked to discover proofs for yourself, often with hints to guide you.

We will try to emphasize preciseness in the stating of definitions and theorems. It often requires a great deal of care to ensure that a statement says precisely what you want it to say. It perhaps seems too obvious to say, but it cannot be stressed too much, that you cannot hope to construct a proof for a statement unless you understand what the statement says and the meanings of all terms in the statement.

OPERATIONS

We often speak of the operations of addition, multiplication, and so forth. What is an operation? To answer this we first observe that the operation addition provides us with a rule whereby we assign to every pair (x, y) of real numbers some other number. Thus, by addition we assign to the pair (2, 3) the sum of the members of the pair, i.e., the number 5. Similarly subtraction assigns the pair (2, 3) to the number ____ and multiplication assigns the same pair to the number ____.

- -

ANSWER:

-1

6.

- -

The usual notation is the following:

$2 + 3 = 5$

$2 - 3 = -1$

$2 \cdot 3 = 6$

Since $2 + 3 = 3 + 2$ and $2 \cdot 3 = 3 \cdot 2$ the order in which the members of the pair (2, 3) are given is immaterial for addition and multiplication. Is this order important for subtraction? Why or why not?

- -

ANSWER:

Yes. $2 - 3 = -1$ but $3 - 2 = 1$, so the result depends upon the order of the members of the given pair.

- -

We would like subtraction to be an example of an operation, which means that the definition must take into account the order of the members of a pair upon which the operation is to act. This leads us to consider ordered pairs. You are already familiar with ordered pairs from Unit I.

Let us again consider the examples:

$2 + 3 = 5$

$2 - 3 = -1$

$2 \cdot 3 = 6$

In each of these examples the operation assigns the ordered pair $(2, 3)$ to a unique number. Using function notation, this can be exhibited as follows:

$(2, 3) \xrightarrow{+}$ ____

$(2, 3) \xrightarrow{-}$ ____

$(2, 3) \xrightarrow{\cdot}$ ____

- -

ANSWER:

5

-1

6

- -

The above discussion leads us to make the following definition.

DEFINITION 2.1: A (binary) operation on a set S is a correspondence which assigns each ordered pair of elements of the set S to a unique element of some set.

In other words, an operation on S is a ____ whose domain is the ____ of elements of S. (Be careful.)

- -

ANSWER:
function
set of ordered pairs

- -

Recall from Unit I that the set of all ordered pairs of elements of S is called the ____ and is denoted by S × S.

- -

ANSWER:
Cartesian product of S with S.

- -

The operation of addition of real numbers is a function of "*two real* variables" because its domain is a set of ____ of ____.

- -

ANSWER:
ordered pairs
real numbers.

- -

DEFINITION 2.2: If an operation "o" assigns each ordered pair of elements of S (i.e., each element of S × S) to an element *in S* we say "o" is a *closed operation* on the set S.

In other words, a closed operation on a set S is a function from ____ to ____.

- -

ANSWER:

$S \times S$

S.

- -

If we add two positive integers, is the sum always a positive integer?

- -

ANSWER:

Yes.

- -

Since addition assigns each ordered pair of positive integers to a positive integer, we can say that addition is a ____ binary operation on the set of positive integers.

- -

ANSWER:

closed

- -

Is subtraction a closed operation on the set of positive integers?

- -

ANSWER:

No; for example, 2 and 7 are positive integers, but $2 - 7 = -5$ and -5 is not a positive integer.

- -

A closed operation on a set is a function whose range is ____.

- -

ANSWER:

a subset of (or is contained in) the given set.

- -

Suppose "o" is a closed operation on a set S. Then for each a and b in S, $(a, b) \xrightarrow{o} c$, where c is in S.

If the operation "o" were not closed, what part of the above statement would be different?

- -

ANSWER:

c would not necessarily be in S.

- -

Since "o" is a function, if we are given (a, b) we know that the element c paired with it is uniquely determined. Is it also true that if c is known, (a, b) is uniquely determined?

- -

ANSWER:

No.

- -

For example, if $a \circ b = c$ and if "o" is the addition operation on the set S of positive integers, then (1, ___) and (3, ___) are different ordered pairs which correspond to c = 5.

- -

ANSWER:

(1, 4)
(3, 2)

- -

This example shows that the addition operation on the set S of positive integers is not a(n) ____ function from S × S to S.

- -

ANSWER:

reversible

- -

Before proceeding further we should make some remarks about the meaning of the equals sign. In this course we will use the symbol "=" to mean "is" or "is the same as". Thus, when applied to real numbers, the statement $a = b$ means that the real number represented by a is the same as the real number represented by b.

Three important consequences of this definition of equality are listed below. We will state these properties for equality of real numbers.

1. If a is a real number, then $a = a$.
2. If a is a real number and b is a real number and $a = b$, then $b = a$.
3. If each of a, b, and c is a real number and if $a = b$ and $b = c$, then $a = c$.

Property 3 above is just the usual substitution rule for equality.

We will use these basic properties of equality in proofs without mentioning them explicity. It would be unnecessarily tedious to have to state them as reasons each time we wished to replace a symbol for a number by a different symbol for the same number, i.e., "to substitute one quantity for an equal quantity". Occasionally, for the sake of clarity, we will give "substitution" as a reason when one or more of these properties of equality are used.

Two other familiar properties relate equality of real numbers to the operations of addition and multiplication.

i. If equals are added to equals, the sums are equal. Thus, if a, b, c, and d are real numbers and if $a = b$ and $c = d$, then $a + c = b + d$.

ii. If equals are multiplied by equals, the products are equal. Thus, if a, b, c, and d are real numbers and if $a = b$ and

7

$c = d$, then $a \cdot c = b \cdot d$.

These properties follow from the meaning of equality and the assumption that addition and multiplication, respectively, are binary operations (functions). If a, b, c, and d are real numbers and $a = b$ and $c = d$, then $(a, c) = (b, d)$; that is, (a, c) and (b, d) are different names for the same ordered pair of numbers. The operation of addition associates (a, c) with the real number $a + c$ and (b, d) with the real number _____.

- -

ANSWER:

$b + d$.

- -

We know since addition is a function that the ordered pair $(a, c) = (b, d)$ is associated with only one number.

Therefore, $a + c = b + d$.

A similar argument would establish the above multiplication property.

We will generally use these properties in proofs without explicitly listing them as reasons.

PROPERTIES OF REAL NUMBER OPERATIONS

In this section we will pick out a few of the basic properties of the real number operations addition and multiplication. These basic properties will be assumed as postulates for the real number system. In later sections we will derive other properties on the basis of the assumed postulates. Be careful to note that the postulates are basic assumptions and that we make no attempt to give proofs for them. You may feel that some of the properties which we will proves as theorems are just as basic as some of the postulates. This may be true. There is always some arbitrariness in the selection of the properties which will be taken as postulates. However, we will choose a set of postulates which does not have needless duplication and which will permit a fairly easy development of all the most important properties of real number addition and multiplication.

We will now discuss these properties informally before stating them as postulates.

THE COMMUTATIVE PROPERTY: For real numbers a, b, and c, if we know that $(a, b) \xrightarrow{+} c$ then it follows that $(b, a) \xrightarrow{+}$ ____.

- -

ANSWER:

c.

- -

Are there similar true statements for any of the other three operations on real numbers, subtraction, multiplication, and division? If so, state them.

- -

ANSWER:

There is a similar statement for multiplication. For real numbers a, b, and c, if $(a, b) \xrightarrow{\cdot} c$, then $(b, a) \xrightarrow{\cdot} c$.

- -

A counter-example which demonstrates that a statement similar to the above is not true for subtraction is the following: $(2, 7) \xrightarrow{-} -5$ and $(7, 2) \xrightarrow{-} 5$. Division also fails to have this property.

The foregoing property, which is possessed by addition and multiplication, is called the commutative property. The commutative property for addition states that $a + b = b + a$, for all real numbers a and b.

THE ASSOCIATIVE PROPERTY: Addition has been assumed to be a binary operation. This means addition is an operation whose domain is a set of ____.

- -

ANSWER:

ordered pairs of elements (real numbers).

How could you indicate the sum of the three numbers 2, 5, and 3, keeping in mind that addition is a binary operation?

ANSWER: $(2 + 5) + 3$ or $2 + (5 + 3)$.

To clarify the meaning of $(2 + 5) + 3$ we use function notation.

$$(2, 5) \xrightarrow{+} 2 + 5$$

$$(2 + 5, 3) \xrightarrow{+} (2 + 5) + 3$$

From our experience we know that $(2 + 5) + 3 = 2 + (5 + 3)$. The difference between the two expressions is only in the choice of the pair to be added first. The property involved here, which is called the associative property of addition, can be stated as follows:

For any real numbers a, b, and c, $(a + b) + c = a + (b + c)$. Note that the order of the terms is not changed.

Because of the associative property of addition there is no ambiguity in writing $a + b + c$ without parentheses. Then, by definition, $a + b + c = (a + b) + c$.

How could you similarly assign a meaning to $a + b + c + d$, for real numbers a, b, c, and d?

ANSWER:

$a + b + c + d = (a + b + c) + d$, where $a + b + c = (a + b) + c$. There are other correct answers, e.g., $(a + b) + (c + d)$.

By an extension of this idea, the sum of any finite sequence of numbers can be defined. The associative property of addition could be used to show that the grouping of the numbers in a sequence does not affect the sum of the numbers in the sequence. For example, for the sequence (a, b, c, d) we have

$$((a + b) + c) + d = (a + b) + (c + d) = a + (b + (c + d)) =$$
$$(a + (b + c)) + d = a + ((b + c) + d).$$

Give a statement of the associative property for each of the other three basic real number operations *for which the property is valid*.

- -

ANSWER:

The property is not valid for subtraction or division. For multiplication it can be stated:

For any real numbers a, b, and c, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

- -

THE DISTRIBUTIVE PROPERTY: We will now turn our attention to a property which relates addition and multiplication. When you write $3x + 5x = 8x$ you make use of this property although many people do so without recognizing it: $3x + 5x = (3 + 5) \cdot x = 8x$.

Is it true for *all* real numbers a, b, and c that $(b + c)a = (b \cdot a) + (c \cdot a)$?

- -

ANSWER:

Yes.

- -

Is it also true that $a(b + c) = (a \cdot b) + (a \cdot c)$ for all real numbers a, b, and c?

- -

ANSWER:

Yes.

- -

Other statements similar in form to the one given above include the following:

(1) $a(b - c) = (a \cdot b) - (a \cdot c)$

(2) $(b - c)a = (b \cdot a) - (c \cdot a)$

(3) $a + (b \cdot c) = (a + b) \cdot (a + c)$

(4) $(b + c) \div a = (b \div a) + (c \div a)$

Which of the above statements are true for all real numbers a, b, and c?

- -

ANSWER:

1, 2. Statement (4) is meaningless if $a = 0$, but it is true if $a \neq 0$.

- -

The two properties $a(b + c) = (a \cdot b) + (a \cdot c)$ and $(b + c)a = (b \cdot a) + (c \cdot a)$ for all real numbers a, b, and c are ordinarily combined and called the distributive property of multiplication over addition.

Many texts in high school algebra will say that for a real number x, $3x + 5x = 8x$ is "combining like terms" and give no indication that the distributive property is involved. Similarly, in writing expressions like $3xy$ no mention is made of the associative property of multiplication. This is even done in some books which are careful to use the distributive and associative properties in other situations, and here it can be a real source of confusion for the student. He is likely to get the idea that the distributive property and "combining like terms" are unrelated ideas.

Consider the following discussion quoted from a well known high school Algebra I text.

> "You will recall that in arithmetic you can add 5 pencils to 2 pencils and obtain 7 pencils as the sum, because you are combining two groups of like things. Similarly, in algebra we can add the term $5x$ to the term $2x$ and obtain $7x$ as the sum --- that is, $5x + 2x =$

$7x$ --- because we are combining two *like terms*. *Like terms* are those which have the *same literal factors*. Thus $4y$ and $9y$ are like terms, and so are ab and $6ab$.

You know that we cannot add 6 pencils to 3 hours and obtain a total of pencils or a total of hours because these are two groups of *unlike* things. Similarly, we cannot add $6x$ and $3n$ (except to indicate the sum as $6x + 3n$), because these are *unlike terms*. *Unlike terms do not* have the same literal factors. Thus $4c$, $5a$, $5y$, x, x^2, and xy are all unlike terms."

The above paragraphs are illustrated as follows.

"3 nails and 4 nails make a total of 7 nails. $3n + 4n = 7n$. Like terms can be combined."

Beneath a picture of 3 bricks and 4 nails is the caption: "All I can say here is 3 bricks and 4 nails. $3b + 4n$. Unlike terms cannot be combined."

It is difficult to imagine a more misleading discussion of a basic algebraic property than that quoted above. If there is anything that should be made perfectly clear to a student concerning addition, it is that we add *numbers*, not pencils or hours or nails or bricks. When we write an expression in algebra like $3b + 4n$ it is almost always with the understanding that the letters b and n are used to stand for *numbers*, not bricks and nails. To say that we can add $3n + 4n$ but cannot add $3b + 4n$ is utter nonsense and cannot help but be misleading to the student. If b and n stand for numbers then we can certainly add $3b + 4n$ as well as $3n + 4n$. What is true, of course, is that the distributive property can be applied to $3n + 4n$ to get $3n + 4n = (3 + 4)n = 7n$ while the distributive property does not apply in the same way to $3b + 4n$ unless $b = n$.

You may feel that the commutative and associative properties of addition and multiplication and the distributive property are intuitively obvious. Your feeling can perhaps be justified, when the numbers involved are positive integers, on the basis of counting notions. However, you might try to formulate in your mind reasons why the following statements should be intuitively obvious:

(a) $\sqrt{2} \cdot \pi = \pi \cdot \sqrt{2}$

(b) $\sqrt{2} \cdot (\pi + 3) = \sqrt{2} \cdot \pi + \sqrt{2} \cdot 3$.

IDENTITY ELEMENTS: The number zero behaves in a special way relative to the addition operation. Thus, if a is any real number then we know that for the ordered pairs (a, 0) and (0, a) we have

$(a, 0) \xrightarrow{+}$ ____

$(0, a) \xrightarrow{+}$ ____.

- -

ANSWER:

a

a

- -

We call zero the identity element for addition or the additive identity element. The identity property for addition is given in the following statement.

There is a real number, 0, such that $a + 0 = 0 + a = a$ for each real number a.

This statement will be one of our postulates for the real number system. The number zero also behaves in a special way relative to the multiplication operation. Thus $a \cdot 0 = 0 \cdot a = 0$ for each real number a. We will not take this statement as one of our postulates since it can be proved easily from the other postulates which we will assume.

There is also an identity element for multiplication. Using the identity property for addition as stated above as a guide, state the identity property for multiplication.

- -

ANSWER:

There is a real number, 1, such that $a \cdot 1 = 1 \cdot a = a$ for each real number a.

- -

This property will also be one of our postulates. We will add to this property the assumption that $1 \neq 0$. This is done for a technical reason which we will not go into here.

INVERSE ELEMENTS: Each of the operations, addition and multiplication, assigns to any given real number many ordered pairs. For example, (2, 5), (3.75, 3.25), and (7/11, 6 4/11) are all assigned to 7 by the ____ operation.

- -

ANSWER:
addition

- -

Consider the pairs which are assigned to 0, the additive identity, by the addition operation. If 4 is the first member of such a pair, the second member of the pair is ____.

- -

ANSWER:
-4.

- -

If the first member of the pair assigned to 0 by addition is $-\sqrt{2}$, then the second member is ____.

- -

ANSWER: $\sqrt{2}$.

- -

When a pair of real numbers (a, b) is assigned to 0 by addition we call b the additive inverse of a and a the additive inverse of b. Since $(4, -4) \xrightarrow{+} 0$, -4 is called the additive inverse of

____, and 4 is called the additive inverse of ____.

- -

ANSWER:

4,

-4.

- -

The numbers ordinarily used in elementary arithmetic are the positive integers, (or natural numbers). When the negative integers are first introduced in algebra it is assumed that for each positive integer n there is an integer $-n$ with the property that $n + (-n) = 0$. $-n$ is then called a negative integer. It is unfortunate that in many high school algebra texts the introduction of the negative integers is accompanied by a statement like the following: "A negative number is a number which has a minus sign attached."

What the author means of course is that if a minus sign is "attached" to one of the numbers of elementary arithmetic, i.e., one of the positive integers, then a negative number is obtained. However, if a minus sign is "attached" to a negative number. then a positive number is obtained. Thus, for example, if a represents the real number which is a solution of the equation $x^3 = -2$, and if we "attach" a minus sign to a, then we obtain a positive number.

The primary use of the minus sign is to indicate the additive inverse of a number, and later to indicate subtraction. If a denotes a number then $-a$ denotes the number which is the additive inverse of a. Be careful not to think of "$-a$" as a symbol for a negative number. $-a$ can be positive, negative, or zero, depending upon the number a.

The inverse property of addition of real numbers can be stated as follows: For each real number a there exists a real number, designated by $-a$, such that $a + (-a) = (-a) + a = 0$.

The corresponding special pairs under multiplication would be those which are assigned to ____.

ANSWER:

1 (the multiplicative identity).

An example of one such pair is (___, 4).

ANSWER:

1/4

Is it true for all real numbers a that $(1/a, a) \xrightarrow{\cdot} 1$?

ANSWER:

No, it is not true for $a = 0$.

But for each non-zero real number a, it is true that $(1/a, a) \xrightarrow{\cdot} 1$.

We will usually represent the multiplicative inverse of a by the symbol "a^{-1}" instead of "1/a."

Formulate a statement of the inverse property of multiplication of real numbers (recalling that 0 has no mulitiplicative inverse).

ANSWER:

For each real number a, $a \neq 0$, there exists a real number, designated by a^{-1}, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. (Note that it is not sufficient to say just "$a \cdot a^{-1} = a^{-1} \cdot a$." You must add " = 1."

We are now ready to state the properties we have discussed as postulates for the real number system. This list of postulates contains three sets of properties:

(1) properties concerning addition,

(2) properties concerning multiplication, and

(3) a property concerning both addition and multiplication.

These properties are called the field properties of the real number system.

We assume that we have a set R called the real number set upon which are defined two closed binary operations, addition and multiplication, having the following properties:

Names of the Properties

Associative

Addition Properties

A_a : For all a, b, c in R, $(a + b) + c = a + (b + c)$.

Multiplication Properties

M_a : For all a, b, c in R, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Commutative

A_c : For all a, b in R, $a + b = b + a$.

M_c : For all a, b in R, $a \cdot b = b \cdot a$.

Identity

A_{id} : R contains an element 0 such that $a + 0 = 0 + a = a$ for all a in R.

M_{id} : R contains an element $1 \neq 0$ such that $a \cdot 1 = 1 \cdot a = a$ for all a in R.

Inverse

A_{in} : For each a in R there exists $-a$ in R such that $a + (-a) = -a + a = 0$.

M_{in} : For each a in R, $a \neq 0$, there exists a^{-1} in R such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Addition and Multiplication

Distributive

D : For all a, b, c in R, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, and $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$.

Note: A shorthand notation has been introduced for the above properties and will be used in the remainder of the course. For example, A_c designates the commutative property for addition, M_{in} designates the inverse property of multiplication while D designates the distributive property of multiplication over addition.

Note carefully the similarity of the properties A_a, M_a; A_c, M_c; A_{id}, M_{id}; and A_{in}, M_{in}.

FIELD THEOREMS FOR THE REAL NUMBER SYSTEM

Having chosen the set of postulates we will now begin to prove theorems giving additional properties of the real number system. As has been previously noted, most of the properties will be well known to you, and you may feel it is unnecessary to prove these as theorems, but you should recall that our purpose in this unit is to examine the basic structure underlying these well-known properties. This is best accomplished by examining the logical dependence of the properties upon one another. In carrying out these proofs we must be careful to use only the postulates we have laid down, together with the theorems which we will have already proved.

THEOREM 2.1a: If a, b, and x are real numbers and $a + x = b + x$, then $a = b$.

Starting with the hypothesis $a + x = b + x$ we can add ____ to $a + x$ and $b + x$ to arrive at the equality of a and b.

- -

ANSWER:

$-x$

- -

We will write this proof in a form that is often used for proofs in high school geometry. Give the symbol for the property applying to steps 4, 5, and 6.

PROOF:

1.	$a + x = b + x$	1.	Hypothesis
2.	$-x$ exists	2.	A_{in}
3.	$(a + x) + (-x) = (b + x) + (-x)$	3.	Note: At this point in the proof the authority, "If equals are added to equals, the sums are equal" could be supplied; but, as was previously explained, we will ordinarily make use of this property without comment.
4.	$(a + x) + (-x) = a + [x + (-x)]$	4.	____
5.	$= a + 0$	5.	____
6.	$= a$	6.	____
	Similarly		
7.	$(b + x) + (-x) = b$		
8.	$\therefore a = b$		

- -

ANSWER:

4. A_a
5. A_{in}
6. A_{id}

- -

In the above proof, the statements (4), (5), and (6) should be thought of as a series of equal expressions which could be written as follows: $(a + x) + (-x) = a + [x + (-x)] = a + 0 = a$. In writing proofs, the format, which lists steps in one column and reasons in an adjacent column, permits one to see at a glance just what steps are used in the proof. However, one who has some experience in constructing proofs may prefer to write the proof in paragraph form. The important thing is that a proof should consist of a sequence of statements which will convice the reader that the conclusion of the theorem is a logical consequence of the hypothesis of the theorem and of the postulates which have been assumed. A proof of Theorem 2.1a is given in paragraph form below.

By hypothesis, $a + x = b + x$. Property A_{in} tells us that x has an additive inverse $-x$. If equals are added to equals the sums are equal, therefore $(a + x) + (-x)$ is equal to $(b + x) + (-x)$. Using the property A_a we see that the statement $(a + x) + (-x) = (b + x) + (-x)$ implies that $a + [x + (-x)] = b + [x + (-x)]$. By property A_{in}, $x + (-x) = 0$, hence $a + 0 = b + 0$. Then $a = b$, by property A_{id}.

THEOREM 2.1b: If a, b, and x are real numbers and $x + a = x + b$, then $a = b$.

PROOF: Let $x + a = x + b$. Then by A_c we have $a + x = b + x$, and by Theorem 2.1a, we know $a = b$.

This proof is a good illustration of how a statement can be proved by relating it to a previously proved theorem.

The property of real numbers given in Theorems 2.1a and 2.1b is often called the cancellation property for addition. We will combine these two theorems in the following single theorem.

THEOREM 2.1: If a, b, and x are real numbers and either $a + x = b + x$ or $x + a = x + b$, then $a = b$.

State the analogue for multiplication of Theorem 2.1a.

- -

ANSWER:

THEOREM 2.2a: If a, b, and x are real numbers with $x \neq 0$, and if $a \cdot x = b \cdot x$, then $a = b$.

- -

Note that the condition "$x \neq 0$" is necessary in the statement of Theorem 2.2a. For example, $2 \cdot 0 = 3 \cdot 0$, but $2 \neq 3$. Look again at the proof of Theorem 2.1a. Each of the basic properties used as reasons in that proof is concerned with addition and each has an analogue for multiplication. In which of the multiplication properties does the condition $x \neq 0$ arise?

ANSWER:

M_{in}

Thus a real number x is assumed to have a(n) ____ only if $x \neq 0$.

ANSWER:

multiplicative inverse

Give a complete proof of Theorem 2.2a (using the proof of Theorem 2.1a for hints, if necessary.) Try to use the same format used in proving Theorem 2.1a.

1. $a \cdot x = b \cdot x$	1. Hypothesis

ANSWER:

1.	$a \cdot x = b \cdot x$	1. Hypothesis
2.	$x \neq 0, \therefore x^{-1}$ exists	2. Hypothesis and M_{in}
3.	$(a \cdot x) \cdot x^{-1} = (b \cdot x) \cdot x^{-1}$	
4i.	$(a \cdot x) \cdot x^{-1} = a \cdot (x \cdot x^{-1})$	4i. M_a
4ii.	$= a \cdot 1$	4ii. M_{in}
4iii.	$= a$	4iii. M_{id}
	Similarly	
5.	$(b \cdot x) \cdot x^{-1} = b$	
6.	$\therefore a = b$	

Note: We use the conventional three dots, $\therefore$, to represent the word "therefore".

- -

You may have written the part of the proof contained in steps 3-6 as follows:

(3) $(a \cdot x) \cdot x^{-1} = (b \cdot x) \cdot x^{-1}$

(4) $a \cdot (x \cdot x^{-1}) = b \cdot (x \cdot x^{-1})$ M_a

(5) $a \cdot 1 = b \cdot 1$ M_{in}

(6) $a = b$ M_{id}

This proof is also correct but you should be careful to note exactly how the reasoning progresses from step to step. For example, a more complete description of the reasoning involved in going from step 3 to step 4 is as follows: By Property M_a we know that $(a \cdot x) \cdot x^{-1} = a \cdot (x \cdot x^{-1})$ and $(b \cdot x) \cdot x^{-1} = b \cdot (x \cdot x^{-1})$. Since, by step 3, $(a \cdot x) \cdot x^{-1} = (b \cdot x) \cdot x^{-1}$, we conclude that $a \cdot (x \cdot x^{-1}) = b \cdot (x \cdot x^{-1})$.

In writing a proof of your own, or in reading a proof, you should always be careful to note exactly how the reasoning proceeds. The proof format that is used should be chosen to make as clear as possible the reasoning involved. There is a proof format often used by students which tends to hide the logic involved in the proof. We will illustrate this format with a very simple example.

EXAMPLE: Prove that if a and b are real numbers and $a + b = 0$, then $(-a) + (-b) = 0$.

PROOF:

$(-a) + (-b) = 0$

$a + [(-a) + (-b)] = a + 0$

$a + [(-a) + (-b)] = a$ A_{id}

$[a + (-a)] + (-b) = a$ A_a

$0 + (-b) = a$ A_{in}

$-b = a$ A_{id}

$(-b) + b = a + b$

$0 = a + b$ $\quad A_{in}$

$0 = 0$ $\quad$ Hypothesis

The proof as given is very misleading. On the surface it appears that one is assuming that $(-a) + (-b) = 0$ and is proving that $0 = 0$. This is, of course, nonsense. We already know that $0 = 0$, and we are trying to prove that $(-a) + (-b) = 0$. The correct argument above is to argue with the given steps in reverse order. A much better way of writing the above proof is as follows:

1. $a + b = 0$ $\quad$ Hypothesis
2. $(-a) + (a + b) = (-a) + 0$
3. $(-a) + (a + b) = -a$ $\quad A_{id}$
4. $[(-a) + a] + b = -a$ $\quad A_a$
5. $0 + b = -a$ $\quad A_{in}$
6. $b = -a$ $\quad A_{id}$
7. $b + (-b) = (-a) + (-b)$
8. $0 = (-a) + (-b)$ $\quad A_{in}$

Here the argument proceeds step by step from the hypothesis (that which is given) to the conclusion (that which is to be proved).

One other comment about reasoning used in proofs. It is bad to develop the habit of regarding multiplication as a form of addition, as, for example, when we say that "$5 \cdot 8 = 40$ means that when we add five 8's we obtain 40." While this is intuitively correct when one of the factors is a positive interger, regarding multiplication in this way leads to such absurdities as "$\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ means that when we add $\sqrt{2}$ many $\sqrt{3}$'s, we obtain $\sqrt{6}$."

THEOREM 2.2b: If a, b, and x are real numbers with $x \neq 0$ and $x \cdot a = x \cdot b$, then $a = b$.

Prove Theorem 2.2b. Use the proof of Theorem 2.1b as a guide.

- -

ANSWER:

Let $x \cdot a = x \cdot b$. Then by M_c we have $a \cdot x = b \cdot x$. Since

$x \neq 0$, we can now conclude that $a = b$ from Theorem 2.2a.

- -

We combine Theorems 2.2a and 2.2b as

THEOREM 2.2: If a, b, and x are real numbers, with $x \neq 0$, and if either $a \cdot x = b \cdot x$ or $x \cdot a = x \cdot b$, then $a = b$.

The property given in Theorem 2.2 is usually referred to as the cancellation property for multiplication.

In proving Theorem 2.1 we did not use any of the postulates which have to do with multiplication. The properties A_a, A_c, A_{id}, and A_{in} are concerned only with addition. Theorem 2.2 is a theorem for multiplication which is almost an exact analogue of Theorem 2.1. The only difference is the added restriction that $x \neq 0$, which is required because of this restriction in Property M_{in}. The proof of Theorem 2.2 is based on properties M_a, M_c, M_{id}, and M_{in} which are multiplication properties and are connected with addition only in an incidental way, viz. in Property M_{id} there is the condition $1 \neq 0$ and in M_{in} there is the restriction $a \neq 0$. (The number 0 is defined by Property A_{id} which is an addition property.)

It is more important that you understand the relationship between Theorems 2.1 and 2.2 than that you memorize the steps in these proofs.

In the introduction to the field properties we observed that the pair $(a, 0)$, where a is any real number, is assigned to 0 by multiplication. It was stated at that time that this could be proved by use of the chosen field postulates, and we will do this now.

THEOREM 2.3: If x is a real number, $x \cdot 0 = 0 \cdot x = 0$.

How is addition involved in the statement of Theorem 2.3?

- -

ANSWER:

The definition of the number 0 involves addition; i.e., 0 is the identity element for addition.

- -

Thus we have an element with a special property under addition appearing in a statement concerning multiplication. This suggests that we should expect to use property ____ in the proof of this theorem.

- -

ANSWER:
distributive, or D. (This is the property which gives a real tie-up between the two operations, addition and multiplication.)

- -

Give three ways that you can substitute in the equation $a(b + c) = (a \cdot b) + (a \cdot c)$ to get an equation in which $x \cdot 0$ appears.

- -

ANSWER:

1. $x(0 + c) = (x \cdot 0) + (x \cdot c)$; substitute x for a and 0 for b.
2. $x(b + 0) = (x \cdot b) + (x \cdot 0)$; substitute x for a and 0 for c.
3. $x(0 + 0) = (x \cdot 0) + (x \cdot 0)$; substitute x for a and 0 for b and for c.

- -

A proof of Theorem 2.3 can be based on any one of these three equations. We will outline a proof using equation 3.

In the statement $x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$ we observe that $x \cdot (0 + 0)$ can be replaced by a simpler expression, namely ____.

- -

ANSWER:
$x \cdot 0$.

- -

The authority for this replacement is ____.

ANSWER:

A_{id}

Thus, we have $x \cdot 0 = (x \cdot 0) + (x \cdot 0)$. You would like to use the cancellation Theorem 2.1 at this point to conclude the proof. Does this statement fit the form of the cancellation theorem for addition?

ANSWER:

No.

How can you alter the statement "$x \cdot 0 = (x \cdot 0) + (x \cdot 0)$" so that you can use Theorem 2.1 to obtain $0 = x \cdot 0$? (If you are going to "cancel" $x \cdot 0$ from both sides to obtain $0 = x \cdot 0$, what form must the left side have before cancellation?)

ANSWER:

$$(x \cdot 0) + 0 = (x \cdot 0) + (x \cdot 0)$$

or $0 + (x \cdot 0) = (x \cdot 0) + (x \cdot 0)$

The property used to justify this change is ____.

ANSWER:

A_{id}

Then by Theorem 2.1 we obtain $0 = x \cdot 0$, or $x \cdot 0 = 0$. Thus, the proof can be stated as follows: By Property D we have $x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$. Since $0 + 0 = 0$, by A_{id}, it follows that $x \cdot 0 = (x \cdot 0) + (x \cdot 0)$. Again we can use Property A_{id} to obtain $(x \cdot 0) + 0 = (x \cdot 0) + (x \cdot 0)$ which, by Theorem 2.1, implies $0 = x \cdot 0$, or $x \cdot 0 = 0$. By Property M_c, we also conclude $0 \cdot x = 0$.

In the proof we have used the fact that if $0 = x \cdot 0$ then $x \cdot 0 = 0$. Is this an application of property M_c?

- -

ANSWER:

No. The order of the factors in the product $x \cdot 0$ is not changed. The property used is one of the basic facts about equality: if a and b are real numbers and $a = b$, then $b = a$.

- -

Instead of proving Theorem 2.3 we could have taken it as one of our postulates. The fact that we can prove it on the basis of our other postulates is not of greatest importance here. What is important however is the fact that this result, in marked contrast to Theorems 2.1 and 2.2, is intimately tied up with both the operations addition and multiplication.

Without giving sufficient thought to the problem, a student would very likely say that Theorem 2.3 is a multiplication theorem. Having gone through the proof here you should have a much clearer idea of the relation of the result to both addition and multiplication.

You will find that when we have a theorem that is additive in nature there is almost always a multiplicative analogue. But if a theorem is essentially tied up with both operations there is no such analogue. (An analogous statement can be obtained by interchanging the roles of the two operations, but the statement so obtained is usually not true.)

Consider the equation $[x + (-2)] \cdot [x + (-3)] = 0$. To solve this equation we say that either $x + (-2) = 0$ or $x + (-3) = 0$, so that either $x = 2$ or $x = 3$. For the equation $[x + (-2)] \cdot [x + (-3)] = 1$, can we conclude that either $x + (-2) = 1$ or $x + (-3) = 1$?

- -

ANSWER:

No.

- -

Do you think you could explain clearly to another student why we can make the first conclusion above but not the second? Try to formulate in your mind such an explanation. (You need not write any answer to this question.)

- -

Does Theorem 2.3 permit us to conclude that $x = 2$ and $x = 3$ are solutions of the equation $[x + (-2)] \cdot [x + (-3)] = 0$?

Does Theorem 2.3 permit us to conclude that $x = 2$ and $x = 3$ are the only solutions of the equation $[x + (-2)] \cdot [x + (-3)] = 0$?

- -

ANSWER:

Yes. (If $x = 2$ or $x = 3$ then one of the factors $x + (-2)$ and $x + (-3)$ is 0; hence, by Theorem 2.3, the product is 0.)

No.

- -

In order to conclude that $x = 2$ and $x = 3$ are the only solutions of the equation $[x + (-2)] \cdot [x + (-3)] = 0$, we need to know that the product $[x + (-2)] \cdot [x + (-3)]$ is 0 only if one of the factors is zero. This is provided by the following theorem.

THEOREM 2.4: If a and b are real numbers and $a \cdot b = 0$, then $a = 0$ or $b = 0$.

If we were to assume in the beginning, that $a = 0$, then there would be nothing to prove. If we assume that $a \neq 0$, then we must prove that ____.

- -

ANSWER:

$b = 0$.

- -

The hypothesis of the theorem tells us that a and b are real numbers and ____.

- -

ANSWER:

$a \cdot b = 0$

- -

One of our postulates tells us something about a real number a under the restriction that $a \neq 0$. Which postulate is it?

- -

ANSWER:

M_{in}

- -

Using the fact that $a \cdot b = 0$ and that a^{-1} exists, prove that $b = 0$. Give a reason for each step in your proof. Be careful to show exactly how property M_a is used.

- -

ANSWER:

1.	$a \cdot b = 0$ and a^{-1} exists	Hypothesis
2.	$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0$	
3.	$(a^{-1} \cdot a) \cdot b = a^{-1} \cdot 0$	M_a
4.	$1 \cdot b = a^{-1} \cdot 0$	M_{in}
5.	$b = a^{-1} \cdot 0$	M_{id}

6. $b = 0$ Theorem 2.3

A proof can also be given based on the cancellation property for multiplication, Theorem 2.2. It is outlined as follows:

$a \cdot b = 0$ and $a \neq 0$, by hypothesis. $a \cdot 0 = 0$ by Theorem 2.3. Hence we have $a \cdot b = a \cdot 0$ and $a \neq 0$. By Theorem 2.2, $b = 0$.

As indicated earlier, the properties contained in Theorems 2.3 and 2.4 are basic to the solution of equations in factored form. Make sure that you understand the roles played by these two theorems in the solution of such equations.

In the equation $[x + (-a)] \cdot [x + (-b)] = 0$, we know that if x is a solution then either $x + (-a) = 0$ or $x + (-b) = 0$, by Theorem ____. Hence $x = a$ and $x = b$ are the only possible solutions. If $x = a$ then $x + (-a) = 0$ and if $x = b$ then $x + (-b) = 0$. Then Theorem ____ tells us that in either case $[x + (-a)] \cdot [x + (-b)] = 0$, so that $x = a$ and $x = b$ are indeed solutions.

ANSWER:

2.4

2.3

Assuming that a and b are real numbers, Theorems 2.3 and 2.4 can be restated as follows:

THEOREM 2.3: If $a = 0$ or $b = 0$ then $a \cdot b = 0$.

THEOREM 2.4: If $a \cdot b = 0$ then $a = 0$ or $b = 0$.

These statements are related in a special way. We can change one statement into the other by interchanging the hypothesis and conclusion. We say that 2.4 is the converse of 2.3 and that 2.3 is the converse of 2.4. The converse of a statement is obtained by interchanging the hypothesis (or assumed part) and the conclusion (or part to be proved).

The additive inverse of a real number a is a real number p such that $a + p = 0$. Postulate A_{in} tells us that every number a has an additive inverse, which we have denoted by $-a$. However A_{in} does not tell us whether a real number a might have more than one additive inverse. The next theorem tells us that it has only one.

THEOREM 2.5: The additive inverse of a real number is unique.

PROOF: Suppose each of the numbers p and q is an additive inverse for the number x. We wish to show that $p = q$.

If p is an additive inverse of x, $x + p =$ ____.

Similarly if q is an additive inverse of x, ____.

- -

ANSWER:

0.

$x + q = 0$.

- -

$\therefore$ ____ $=$ ____, since each expression equals zero.

- -

ANSWER:

$x + p = x + q$

- -

$p = q$ by ____.

- -

ANSWER:

the cancellation property for addition, Theorem 2.1.

- -

There are often many different ways to state a theorem without altering its essential meaning. For example, Theorem 2.5 might be restated as follows:

If a and p are real numbers and $a + p = 0$ then $p = -a$.

The proof we have given for Theorem 2.5 might then be rewritten as follows:

$-a$ is a number such that $a + (-a) = 0$, by A_{in}. Also $a + p = 0$, by hypothesis.

Thus $a + p = a + (-a)$. By Theorem 2.1, $p = -a$.

THEOREM 2.6: The multiplicative inverse of a non-zero real number is unique. Prove Theorem 2.6. (Use the proof of Theorem 2.5 as a guide.)

- -

ANSWER:

Suppose each of the numbers p and q is a multiplicative inverse for the non-zero real number x. Then $x \cdot p = 1$ and $x \cdot q = 1$. Therefore $x \cdot p = x \cdot q$. Since $x \neq 0$, $p = q$ by Theorem 2.2.

- -

We can prove in a similar way that the additive identity and multiplicative identity are unique, but we will not do so now.

MODULAR ARITHMETICS

There are, in addition to the system of real numbers, many mathematical systems which are formed from sets with one or more binary operations. Before proceeding with our development of the real number properties we will take a look at a few of these systems. Although these systems are important in mathematics in their own right, our purpose in introducing them here is to help you to better understand the real number properties. The systems which we will study have many properties in common with the real number system, and their very unfamiliarity should force you to think more clearly about the real number properties.

The first example will be constructed from the set of the first twelve positive integers. These are the numbers which usually appear on the face of a clock. The system that we will build is often called the clock arithmetic. If we picture the positive integers 1, 2, ..., 12 as they appear on the face of a clock we find that there is a natural way to define an addition operation for these integers. We will illustrate with some examples.

To add $2 + 5$, we start at the number 2 on the clock face and count in a clock-wise direction 5 units, arriving at 7. So $2 + 5 = 7$ in this arithmetic just as in the arithmetic of real numbers.

To add $9 + 6$, we start at the number 9 on the clock face and count in a clock-wise direction 6 units, arriving at 3. So $9 + 6 = 3$ in this arithmetic, which is different from $9 + 6$ in the arithmetic of real numbers.

In the clock arithmetic, we have

$8 + 5 =$ ____

$1 + 7 =$ ____

$12 + 2 =$ ____

- -

ANSWER:

1

8

2

- -

Let S be the set $\{1, 2, 3, ..., 12\}$ of the first twelve positive integers. It is clear from the way that addition is defined in the clock arithmetic that if a and b are any numbers in the set S, then $a + b$ is also a number in the set S. Therefore addition in the clock arithmetic is a ____ operation on the set S.

- -

ANSWER:

closed.

- -

If we take any number a in the set S, we have

$12 + a =$ ____

$a + 12 =$ ____.

- -

ANSWER:

a

a.

- -

The number 12 in the clock arithmetic behaves with respect to addition like what number in the arithmetic of real numbers?

- -

ANSWER:

the number 0.

- -

In other words, 12 is an identity element for addition in the clock arithmetic. For the clock arithmetic we have, therefore, a property like Property A_{id} which we have assumed for real number arithmetic. It can be stated as follows:

A_{id}: There is an element 12 in S such that $12 + a = a + 12 = a$ for each a in S.

In the clock arithmetic an additive inverse of an element a in S would be an element b in S such that $a + b = b + a =$ ____.

- -

ANSWER:

12. (a + b) must be the identity element for addition, which in the clock arithmetic is 12.)

- -

Thus the additive inverse of 5 is 7 because $5 + 7 = 7 + 5 = 12$.

What is the additive inverse of 3? ____, of 1? ____, of 12? ____.

- -

ANSWER:

9

11

12 (0 is not correct, because 0 is not in S.)

- -

It should now be clear that each element of S has an additive inverse in the clock arithmetic. So the clock arithmetic has a property analogous to the property A_{in} which we have assumed for the arithmetic of real numbers. It is also true, and not difficult to show, that addition in the clock arithmetic has the associative and commutative properties.

Therefore we see that on the set S we have a closed binary operation, addition, such that properties A_a, A_c, A_{id}, and A_{in} are valid.

We now introduce a system which is essentially the same as the clock arithmetic, but in which we will also define a multiplication operation.

The system which we are going to discuss will be denoted by I/12 and will be called the arithmetic modulo 12. Instead of the set $S = \{1, 2, 3, \ldots, 12\}$ we take $I/12 = \{0, 1, 2, \ldots, 11\}$; i.e., we simply replace the number 12 by the number 0. We define addition in I/12 just as it was defined in the clock arithmetic except that whenever 12 occurs we replace it by 0. Thus, for example, in I/12 we have $8 + 3 = 11$, $9 + 5 = 2$, $8 + 10 = 6$, but $2 + 10 = 0$, $7 + 5 = 0$, etc. In the clock arithmetic the additive identity was 12; in I/12 the additive identity is ____.

ANSWER:

0

We should again emphasize that the system I/12 is essentially the same as the clock arithmetic; only a change in notation is involved in going from one to the other.

The notation used in I/12 permits us to state the definition of addition in the following way:

If a and b are elements of I/12 (i.e., elements of the set $\{0, 1, 2, \ldots, 11\}$) then $a + b$ is the remainder obtained when the ordinary real number sum $a + b$ is divided by 12. For example the real number sum $3 + 5$ is 8 and when 8 is divided by 12 we get a quotient 0 and remainder 8. So $3 + 5 = 8$ also in I/12.

The real number sum $7 + 9$ is 16 and when 16 is divided by 12 we get a quotient 1 and remainder 4. So $7 + 9 = 4$ in I/12.

We can write down an addition table for I/12. We take twelve rows labeled $0, 1, 2, \ldots, 11$ and twelve columns labeled also $0, 1, 2, \ldots, 11$. Then we put in the row labeled a and the column labeled b the sum $a + b$ in I/12. The addition table for I/12 is given below.

+	0	1	2	3	4	5	6	⑦	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
⑨	9	10	11	0	1	2	3	④	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

To find the sum 9 + 7, for example, you look in the row labeled 9 and the column labeled 7 and you find 4, 9 + 7 = 4. The 4 is encircled in the table.

Before continuing with the discussion of I/12 let us look at a simpler system which is very much like I/12. This new system will be denoted I/3 and will be called the arithmetic modulo 3.

We take I/3 = {0, 1, 2}. If a and b are elements of I/3 we define a + b to be the remainder when the real number sum a + b is divided by 3. Thus the real number sum 1 + 2 is 3 and when 3 is divided by 3 we get a quotient 1 and remainder 0. Hence 1 + 2 = 0 in I/3.

In I/3 what is

0 + 2? ____

2 + 2? ____

2 + 1? ____

- -

ANSWER:

2

1

0

- -

Complete the following addition table for I/3:

+	0	1	2
0	0		2
1			0
2		0	1

- -

ANSWER:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- -

In a similar manner we define multiplication in I/3. If a and b are elements of I/3 then $a \cdot b$ in I/3 is the remainder when the real number product $a \cdot b$ is divided by 3. For example, the real number product $1 \cdot 2$ is 2, and when 2 is divided by 3 we get a quotient 0 and remainder 2. Hence $1 \cdot 2 = 2$ in I/3. Complete the multiplication table for I/3.

·	0	1	2
0	0	0	
1			2
2			

- -

ANSWER:

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- -

The two operations, addition and multiplication, can be described by the use of function notation. For example, in arithmetic modulo three,

$(0, 1) \xrightarrow{+} 1$ $(0, 1) \xrightarrow{\cdot}$ ____
$(1, 2) \xrightarrow{+}$ ____ $(1, 2) \xrightarrow{\cdot}$ ____

- -

ANSWER:

0
0 2

- -

Mathematical systems like I/3 are known as modular arithmetics. This system is called arithmetic modulo three, or simply mod 3. The number 3 is called the modulus of this system.

Is addition mod 3 a closed operation?

- -

ANSWER:

Yes.

- -

In an operation table where will the elements associated with ordered pairs of the form (a, a) be found?

- -

ANSWER:

On the main diagonal (from upper left to lower right) of the table.

- -

What can one say about the relative positions of elements associated with the pairs (a, b) and (b, a) in an operation table?

- -

ANSWER:

They will be found in positions which are symmetric with respect to the main diagonal.

- -

If it is true that $(a, b) \xrightarrow{+} c$ and $(b, a) \xrightarrow{+} c$ (the same element c), for every pair (a, b) in the set, we can conclude that the addition operation has the ____ property.

- -

ANSWER:

commutative

- -

Thus to determine whether or not an operation described by a table is commutative you could check the table to see if it is ____.

- -

ANSWER:

symmetric about the main diagonal.

- -

It is now clear from the tables that addition and multiplication modulo 3 are commutative operations.

Until indicated otherwise, the following items refer to arithmetic modulo 3.

(2 + 1) + 1 = ____ + 1 = ____

2 + (1 + 1) = 2 + ____ = ____

$\therefore$ (2 + 1) + 1 = ____

- -

ANSWER:

0 1

2 1

2 + (1 + 1)

- -

The property of addition mod 3 suggested by the above example is the ____ property.

- -

ANSWER:

associative

- -

In order to prove that addition mod 3 has the associative property what would we have to prove?

- -

ANSWER:

We would have to prove that (a + b) + c = a + (b + c) for all a, b, and c in I/3.

- -

There are 27 cases which would have to be examined in order to exhaust all of the cases for I/3. We will not attempt to examine all of them but we will simply assure you that addition mod 3 is an associative operation.

Which element is the identity element for this operation?

- -

ANSWER:

0

- -

Complete the following list by filling in the blanks.

0 + ____ = 0
1 + ____ = ____ + 1 = 0
2 + ____ = ____ + 2 = 0

- -

ANSWER:

0 + 0 = 0
1 + 2 = 2 + 1 = 0
2 + 1 = 1 + 2 = 0

- -

The above list allows one to conclude the following:

The additive inverse of 0 = ____
The additive inverse of 1 = ____
The additive inverse of 2 = ____

- -

ANSWER:

0
2
1

- -

The symbol we use to designate the additive inverse of a is "-a". Therefore,

-0 = ____

-1 = ____

-2 = ____

ANSWER:

0

2

1

We conclude that addition modulo three has the ____ property. Why?

ANSWER:

additive inverse, or A_{in}. We have demonstrated that corresponding to each element a in I/3, there is an element -a in I/3 such that a + (-a) = -a + a = 0.

Be careful to note in the above that -1 and -2 do not refer to the real number additive inverses of 1 and 2. These numbers are not even in the set I/3. The symbols -1 and -2 refer to the elements of I/3 which are the additive inverses in I/3 of 1 and 2; hence -1 = 2 and -2 = 1 because 1 + 2 = 0 and 2 + 1 = 0 in I/3.

We have shown that addition mod 3 has all of the field properties which characterized real number addition, i.e., A_a, A_c, A_{id}, and A_{in}.

Refer to the multiplication table to test multiplication mod 3.

Is the operation closed? How do you know?

ANSWER:

Yes, because each entry in the multipication table is an element of the set I/3.

Multiplication mod 3 is associative. One way to prove this is to check that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all of the 27 possible ordered triples (a, b, c). You will not be required to do this. We illustrate with a single example.

$(2 \cdot 2) \cdot 1 =$ ____ $\cdot$ ____ $=$ ____.

$2 \cdot (2 \cdot 1) =$ ____ $\cdot$ ____ $=$ ____.

Hence $(2 \cdot 2) \cdot 1 = 2 \cdot (2 \cdot 1)$.

ANSWER:

$1 \cdot 1 = 1$

$2 \cdot 2 = 1$

The identity element in the set I/3 relative to multiplication mod 3 is ____.

ANSWER:

1

Is there an element x in I/3 such that $2 \cdot x = 1$ mod 3? If so, what is it?

ANSWER:

Yes

2

Therefore we conclude that the multiplicative inverse of 2 in I/3 is ____.

- -

ANSWER:

2

- -

As in real number multiplication we denote the multiplicative inverse of an element a in I/3 by a^{-1}. Thus 2^{-1} = ____.

- -

ANSWER:

2

- -

Following a similar line of reasoning fill in the following two blanks.

0^{-1} = ____
1^{-1} = ____

- -

ANSWER:

0^{-1} does not exist since there is no x in I/3 such that $0 \cdot x = 1$. (Note that the answer "0" is not correct.)

1^{-1} = 1.

- -

Does multiplication modulo three satisfy the M_{in} property of real number multiplication?

- -

ANSWER:

Yes. (Recall that 0 was not required to have a multiplicative inverse in property M_{in}.)

- -

Real number arithmetic had one additional property which was included in the list of field properties, namely, the distributive property. For real numbers, multiplication is distributive over addition, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for every a, b, c, in R.

Test each of the following statements in arithmetic mod 3 and check those which are true.

a. $2 \cdot (1 + 1) = (2 \cdot 1) + (2 \cdot 1)$

b. $1 \cdot (2 + 2) = (1 \cdot 2) + (1 \cdot 2)$

c. $1 \cdot (0 + 2) = (1 \cdot 0) + (1 \cdot 2)$

- -

ANSWER:

a. $2 \cdot (1 + 1) = 2 \cdot 2 = 1$

$(2 \cdot 1) + (2 \cdot 1) = 1$

$\therefore 2 \cdot (1 + 1) = (2 \cdot 1) + (2 \cdot 1)$. True.

b. and c. are also true.

- -

One could prove that multiplication is, in fact, distributive over addition in arithmetic modulo three simply by examining all 27 possible cases, or by more elegant methods. Neither will be required here.

Each of the field postulates for the real number system is valid for the arithmetic modulo 3. Hence we say that arithmetic modulo 3 is a field.

If we have any algebraic system in which there are defined two closed binary operations, addition and multiplication, which have the properties A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, M_{in}, and D, then we know that any theorem which we prove for the real numbers on the basis of these postulates will automatically hold for that system. In particular, any such theorem is true for arithmetic modulo 3. This points up one of the advantages of the postulational approach to algebra. In general, suppose one introduces a set of postulates for an algebraic system and proves a number of theorems based on these postulates. Further suppose that the occasion arises for one to study properties of a new system with which he is not familiar. If it should happen that the given postulates can be shown to hold for the new system, then it will immediately follow that all of the theorems which were proved on the basis of the postulates also hold for the new system. There are in fact many systems in algebra for which all of the field postulates that we have assumed for the real numbers are valid. Mathematicians have agreed to call any such system a field. Arithmetic modulo 3 is an example of a field.

Construct addition and multiplication tables for arithmetic modulo 4 (denoted $I/4$). The set is $\{0, 1, 2, 3\}$, and each sum (or product) is expressed as the remainder after the sum (or product) obtained by real number operations is divided by 4. For example, $2 + 2 = 0$ modulo 4 because when 4 is divided by 4 a remainder of 0 is obtained.

ANSWER:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

It can be proved, and it will be proved in a later unit, that addition modulo n and multiplication modulo n are associative operations and that multiplication is distributive over addition, for every positive integer n. Thus you will not be asked to test arithmetic modulo four for these properties. However, in testing arithmetic modulo four for other properties your tests or proofs should be complete.

It is clear from the above addition and multiplication tables that addition and multiplication are closed operations in $I/4$. In fact, the definitions of addition and multiplication in arithmetic modulo n ensure that these operations are closed in I/n, for every choice of n as a positive integer.

Having been given that addition modulo four is closed and has the associative property, determine which additional postulates for real number addition are valid for this operation. (Be sure to write the information required to test these properties.)

You should have checked the commutative, identity and inverse properties. When you have tested all three above-mentioned properties go on to the answer.

ANSWER:

The commutative, identity, and inverse properties are all valid.

The commutative property follows from the symmetry of the table about the main diagonal.

0 is the required identity element. From the addition table,
$0 + a = a + 0 = a$, for each element a in $I/4$.
$-1 = 3 \qquad -3 = 1$
$-2 = 2 \qquad -0 = 0$. Therefore corresponding to each element in $I/4$ there is an inverse which is in $I/4$.

In a similar manner, determine which of the postulates for real number multiplication are valid for multiplication modulo four. (Do not test closure and the associative property.)

- -

Have you tested the commutative, identity, and inverse properties? If so, go on to the answer.

- -

ANSWER:
The commutative and identity properties are held in common. If you included the inverse property in this list go to the next item. If you correctly left the inverse property off this list go to the $\boxed{\dagger\dagger}$ below.

- -

Property M_{in} requires that for every non-zero element a in the set, there exists an element in the set, denoted a^{-1}, such that ____ = 1.

- -

ANSWER:
$a \cdot a^{-1}$ (or $a^{-1} \cdot a$).

- -

Is there an element x in $I/4$ such that $2 \cdot x = 1$?

- -

ANSWER:
No.

- -

Since 2 has no multiplicative inverse and $2 \neq 0$, property M_{in} fails to hold for multiplication mod 4.

$\boxed{\dagger\dagger}$ Arithmetic modulo four satisfies all of the field postulates of real number arithmetic except M_{in}. Since $I/3$ had all of the field properties of real number arithmetic we see that the structure of

I/3 is basically different from that of I/4. Note, however, that the *addition* operations of I/3, I/4, and the real numbers satisfy the same postulates. These properties are the closure, commutative, associative, identity, and inverse properties. Many other mathematical systems have this same set of properties for a single operation. Since so many systems have these properties in common they have been given a common name. This is given in the next section.

DEFINITION OF A GROUP

DEFINITION 2.3: An algebraic system made up of a non-empty set, G, and one *closed* binary operation on G is called a *group* if the following hold:

a. the operation is associative,

b. there is an identity element in G relative to the operation,

c. corresponding to each element in G there is an inverse element in G relative to the operation.

If the operation on G is commutative, the group is called a *commutative group*.

Any system which satisfies this definition has many further properties. If we treat the parts of the definition as postulates, many theorems (such as some of those already proved about real number addition) can be proved on the basis of the postulates. Thus, by studying groups in this abstract form, one discovers facts about many systems at once.

Which of the following mathematical systems are groups?

a. The integers under addition.

b. Real numbers under multiplication.

c. The *positive* rational numbers under multiplication.

Note: You should ask the same kinds of questions as have been asked about addition modulo 3 and 4.

- -

ANSWER:

a.

c.

(Note: b fails since zero has no inverse under multiplication while the definition of a group requires that every element have an inverse.)

- -

We have seen earlier that I/3 is a field, i.e., it satisfies all the field postulates. Is I/4 a field? Explain.

- -

ANSWER:

No, I/4 does not satisfy M_{in}. The non-zero element 2 of I/4 has no inverse under multiplication.

- -

We have previously studied addition in the arithmetic modulo 12, I/12. The multiplication table for this arithmetic is on the following page.

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Multiplication is closed in I/12 and is associative. Using the table answer the following questions.

The table is symmetric about the main diagonal. This shows that the operation has the ____ property.

- -

ANSWER:

commutative

- -

The element ____ is the identity element for multiplication in I/12.

- -

ANSWER:

1

- -

What elements of I/12 have inverse with respect to multiplication modulo 12?

- -

ANSWER:

1, 5, 7, and 11.

- -

It can also be shown that in the arithmetic modulo 12, multiplication is distributive over addition. Hence in I/12 we have two closed binary operations, addition and multiplication, which satisfy all the field postulates except for ____.

- -

ANSWER:

M_{in}.

- -

Later in the course we will return to a discussion of the modular arithmetics. Now we continue our development of the real number properties.

SUBTRACTION AND DIVISION

The field postulates and the theorems so far considered are concerned with the operations addition and multiplication. In this section we will define subtraction and division and consider several theorems related to these operations. Subtraction is defined in terms of addition and division in terms of multiplication.

The statement $b - a = d$ is equivalent to the statement $d + a = b$. We have assumed that for each ordered pair of real numbers (a, b), there is a real number which is their sum. Here we are faced with the question: If we know one member of the ordered pair and the sum, does the other member of the ordered pair exist and is it unique? In function notation we could represent the question this way: $(?, a) \xrightarrow{+} b$. The search for a real number to fit in this position leads to the difference $b - a$. To establish the existence of such a number we construct a real number d such that $d + a = b$. How can d be written using only addition properties?

- -

ANSWER:

$b + (-a)$.

- -

THEOREM 2.7: If a and b are real numbers, there is a unique real number d such that $d + a = b$; and furthermore $d = b + (-a)$.

Part 1: Prove: If $d = b + (-a)$, then $d + a = b$. (Be careful to indicate exactly how the associative property A_a is used. In every step parentheses should be used to indicate which pair of numbers is added first, if addition of more than two numbers is involved.)

- -

ANSWER:

1.	$d = b + (-a)$	1. Hypothesis
2.	$d + a = (b + (-a)) + a$	
3.	$= b + ((-a) + a)$	3. A_a
4.	$= b + 0$	4. A_{in}
5.	$= b$	5. A_{id}
6.	$\therefore\ d + a = b$	

- -

Part 2: Uniqueness of d. Assume there is a real number d and a real number f such that $d + a = b$ and also $f + a = b$. Prove that $d = f$.

- -

ANSWER:

1.	$d + a = b, \quad f + a = b$	1. Hypothesis
2.	$\therefore d + a = f + a$	
3.	$\therefore d = f$	3. Theorem 2.1

In the above uniqueness proof it is not correct to assume that $d = b + (-a)$ and $f = b + (-a)$. This amounts to assuming what you are asked to prove. You can only assume that d and f are such that $d + a = b$ and $f + a = b$. It would be correct, however, to assume that $d + a = b$ and *prove* that $d = b + (-a)$. This would show that any real number d such that $d + a = b$ has to be the (unique) real number $b + (-a)$. This proof could be carried out as follows:

1.	$d + a = b$	Hypothesis
2.	$-a$ exists	A_{in}
3.	$(d + a) + (-a) = b + (-a)$	
4.	$d + [a + (-a)] = b + (-a)$	A_a
5.	$d + 0 = b + (-a)$	A_{in}
6.	$d = b + (-a)$	A_{id}

DEFINITION 2.4: If a and b are real numbers, then $b - a$ is the unique real number d such that $d + a = b$. Alternatively, $b - a = b + (-a)$.

Another connection between addition and subtraction is shown in the following statement:

$(b + a) - a = (b + a) + (-a) =$ ____.

ANSWER:

b

When we add a to b and then subtract a from that sum, the result is b. The operation of subtracting *a* *annuls* the effect of adding a. It is for this reason that subtraction is often referred to as the inverse of addition. Thus, addition and subtraction serve as examples of inverse operations.

The use of the word inverse here is related to its use in connection with functions. Let a be a real number and consider the functions f and g defined by:

$f(x) = x + a$, for each real number x,

$g(x) = x - a$, for each real number x.

f and g are functions with domain the set ____.

- -

ANSWER:

of real numbers.

- -

Let $g \circ f$ denote the composite of g with f. Remember that

$g \circ f: x \longrightarrow g(f(x))$, for each real number x.

Therefore, in our example,

$g \circ f: x \longrightarrow g(f(x)) =$ ____ for each real number x.

- -

ANSWER:

$(x + a) - a = x$.

- -

The function $g \circ f$ is the identity function on the set of real numbers.

Similarly

$f \circ g: x \longrightarrow f(g(x)) =$ ____.

- -

ANSWER:

$(x - a) + a = x$.

- -

So $f \circ g$ is also the identity function on the set of real numbers. Therefore the function g is the ____ of the function f.

- -

ANSWER:

inverse

- -

Next we define division. The statement $b \div a = q$ is to be equivalent to the statement $q \cdot a = b$. Thus we look for a real number q such that $(q, a) \xrightarrow{\cdot} b$. If $a \neq 0$ we can choose $q =$ ____ to get $q \cdot a = b$.

- -

ANSWER:

$b \cdot a^{-1}$

- -

This leads us to the statement of the following theorem.

THEOREM 2.8: If a and b are real numbers and $a \neq 0$, there is a unique real number q such that $q \cdot a = b$; and furthermore $q = b \cdot (a^{-1})$.

Prove that if $q = b \cdot a^{-1}$, then $q \cdot a = b$. (Use the proof of Theorem 2.7 as a guide.)

- -

ANSWER:

1.	$q = b \cdot a^{-1}$	Hypothesis
2.	$q \cdot a = (b \cdot a^{-1}) \cdot a$	
3.	$= b \cdot (a^{-1} \cdot a)$	M_a
4.	$= b \cdot 1$	M_{in}
5.	$= b$	M_{id}
6.	$\therefore q \cdot a = b$	

- -

Prove the uniqueness of q. (Assume that q and r are real numbers and that $q \cdot a = b$ and $r \cdot a = b$. Prove $q = r$. Remember that we are also assuming that $a \neq 0$.)

ANSWER:

1.	$q \cdot a = b, \ r \cdot a = b$	Hypothesis
2.	$q \cdot a = r \cdot a$	
3.	$a \neq 0$	Hypothesis
4.	$q = r$	Theorem 2.2

As in the addition case, we can also prove the uniqueness part of Theorem 2.8 by showing that if $q \cdot a = b$ then q must be the (unique) number $b \cdot a^{-1}$. The proof is as follows:

1.	$q \cdot a = b$ and $a \neq 0$	Hypothesis
2.	a^{-1} exists	M_{in}
3.	$(q \cdot a) \cdot a^{-1} = b \cdot a^{-1}$	
4.	$q \cdot (a \cdot a^{-1}) = b \cdot a^{-1}$	M_a
5.	$q \cdot 1 = b \cdot a^{-1}$	M_{in}
6.	$q = b \cdot a^{-1}$	M_{id}

DEFINITION 2.5: If a and b are real numbers and $a \neq 0$, then $b \div a$ is the unique real number q such that $q \cdot a = b$. Alternatively, $b \div a = b \cdot a^{-1}$.

The quotient $b \div a$ is often denoted by b/a.

Suppose a is a non-zero real number and f and g are functions defined by:

$f(x) = x \cdot a$, for each real number x,

$g(x) = x \div a$, for each real number x.

Then $g \circ f$ is the ____ function on the set of real numbers.

ANSWER:

identity

$f \circ g$ is also the identity function. Hence g is the inverse of the function f. For this reason division is often referred to as the inverse of the operation multiplication.

We observe also that if $a \neq 0$, then

$a/a = a \div a = a \cdot a^{-1} = 1.$

DIVISION BY ZERO: In Theorem 2.8, we assumed that $a \neq 0$. What portion of the proof of the theorem was dependent on the condition $a \neq 0$?

ANSWER: The existence of the multiplicative inverse of a. (This was used explicitly in the first part of the proof. In the second part it was needed in order to be able to apply Theorem 2.2, the cancellation property. The proof of Theorem 2.2 in turn also required the existence of the multiplicative inverse.)

If we were to permit $a = 0$ in the definition of division, we would have $b \div 0 = q$ implies $b = q \cdot 0$.

If $b \neq 0$, is this statement true for some real number q? What theorem can you give as reason?

ANSWER:

No

Theorem 2.3.

If $b = 0$, is the statement $b = q \cdot 0$ true for some real number q?

- -

ANSWER:

Yes, for every real number q.

- -

Thus, if $b = 0$ there is still difficulty in defining $b \div 0$. In this case every real number q satisfies the condition $q \cdot a = b$ of Definition 2.5.

Whether $b = 0$ or $b \neq 0$ we have difficulties in defining $b \div 0$. Hence we just make the agreement that $b \div 0$ has no meaning; division by zero is never permitted.

It is a mistake to try to justify such symbolism as "$b/0 = \infty$ if $b \neq 0$" unless one has the required background in limits (from calculus). Without this background such symbolism can only be confusing. Certainly the student should never be given the idea that the symbol "∞" represents a real number.

The division operation is not defined for all ordered pairs of real numbers; hence it *is not* a binary operation on the set of all real numbers. It is defined for all ordered pairs of *non-zero* real numbers; hence it *is* a binary operation on the set of non-zero real numbers. To prove that division is a closed operation on the set of non-zero real numbers we have to show that if a and b are non-zero real numbers then ____.

- -

ANSWER:

$b \div a$ (or $a \div b$) is a non-zero real number.

- -

Let $q = b \div a$, where $a \neq 0$ and $b \neq 0$. Then $b = q \cdot a$.

Since $b \neq 0$, what theorem permits us to conclude that $q \neq 0$?

- -

ANSWER:

Theorem 2.3. (If we had $q = 0$ then Theorem 2.3 would tell us that $q \cdot a = b$ is zero. But $b \neq 0$. Hence $q \neq 0$. Theorem 2.4 is not a correct answer to this question.)

- -

All of the theorems that we have proved about the real numbers, Theorems 2.1 through 2.8, hold for any field. In particular, these theorems hold for arithmetic modulo 3, I/3. Remember that I/4 and I/12 are not fields; Property M_{in} fails for these systems.

In I/12 we have $8 \cdot 2 = 4$ and $8 \cdot 11 = 4$. Hence $8 \cdot 2 = 8 \cdot 11$. This illustrates the failure of what theorem for I/12?

- -

ANSWER:

Theorem 2.2 - the cancellation property for multiplication.

- -

The proof of Theorem 2.2 depended upon Property M_{in}. Hence there was no reason to expect Theorem 2.2 to hold for I/12. Theorem 2.8 also fails for I/12, so we cannot always define $b \div a$ for a and b in I/12, $a \neq 0$. For example $3 \div 4$ is not defined in I/12 because there is no element c in I/12 such that $4 \cdot c = 3$. However subtraction is defined in each of the modular arithmetics.

REVIEW ITEMS

1. Prove: If a is a real number such that $a \cdot x = x$ for every real number x, then $a = 1$.

Give a reason for each step in your proof.

- -

ANSWER:

There are several ways to prove this. Perhaps the easiest is the following:

PROOF: By M_{id}, $a \cdot 1 = a$. By the hypothesis of the theorem, taking $x = 1$, we have $a \cdot 1 = 1$. Therefore $a = 1$.

---

2. Prove: If a and b are real numbers, $(-a) + b = -(a - b)$. Give a reason for each step in your proof.

ANSWER:

1. $[(-a) + b] + (a - b) = [b + (-a)] + (a - b)$
2. $= [b + (-a)] + a + (-b)$
3. $= \{b + [(-a) + a]\} + (-b)$
4. $= (b + 0) + (-b)$
5. $= b + (-b)$
6. $= 0$
7. $\therefore [(-a) + b] + [a - b] = 0$
8. Therefore $[(-a) + b] = -(a - b)$

1. A_c
2. Definition of subtraction
3. A_a (applied twice)
4. A_{in}
5. A_{id}
6. A_{in}

8. A_{in}, Theorem 2.5

---

3. Let the operation "o" be defined on the real numbers as follows: $a \text{ o } b = a + b + 1$ where "+" is the usual real number addition. (Thus A_a, A_c, A_{id}, and A_{in} hold for "+".)

Prove that "o" is a closed operation on the real number set.

ANSWER:

This simply requires the observation that "$a \text{ o } b$" will be a real number whenever a and b are real numbers since "+" is a closed operation on the real number set. Thus "o" is also a closed operation on the set of real numbers.

Prove that "o" is a commutative operation.

ANSWER:

We must prove $a \text{ o } b = b \text{ o } a$ for all real numbers a and b.

1.	$a \text{ o } b = a + b + 1$	1. Definition of "o"
2.	$= b + a + 1$	2. A_c
3.	$= b \text{ o } a$	3. Definition of "o"
4.	$\therefore a \text{ o } b = b \text{ o } a$	

Prove that "o" is an associative operation. (Reasons are not required.)

ANSWER:

We must prove $(a \text{ o } b) \text{ o } c = a \text{ o } (b \text{ o } c)$ for all real numbers a, b, and c.

By definition, $(a \text{ o } b) \text{ o } c = (a + b + 1) \text{ o } c = (a + b + 1) + c + 1 = a + b + 1 + c + 1$.

By definition, $a \mathbin{o} (b \mathbin{o} c) = a \mathbin{o} (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 1 + 1$.

We have shown above $(a \mathbin{o} b) \mathbin{o} c = a + b + 1 + c + 1$; and by A_c (and A_a) this equals $a + b + c + 1 + 1$. This is equal to $a \mathbin{o} (b \mathbin{o} c)$. Therefore $(a \mathbin{o} b) \mathbin{o} c = a \mathbin{o} (b \mathbin{o} c)$ for all real numbers a, b, and c.

Prove that the identity property holds for this system.

ANSWER:

In order to show that this mathematical system has the identity property we must show that there is a real number e such that $a \mathbin{o} e = e \mathbin{o} a = a$ for all real numbers a.

The equation $a \mathbin{o} e = a$ is equivalent to $a + e + 1 = a$, which is valid only if $e = -1$. By substitution it is easy to check that $a \mathbin{o} (-1) = a$ and $(-1) \mathbin{o} a = a$, for every real number a. Thus -1 is the required identity element.

Prove that every real number a has an inverse under the operation "o".

ANSWER:

Recall that -1 is the identity element. Solve the equation $a \mathbin{o} x = -1$ to find the inverse of a real number a.

Thus
$$\begin{aligned} a \mathbin{o} x = a + x + 1 &= -1 \\ x &= -a - 2 \\ \text{or} \quad x &= -(a + 2) \end{aligned}$$

Having demonstrated that the real number set under the operation "o" has the above properties, we can conclude that this structure may be classified as a(n) ____.

ANSWER:

commutative group.

---

4. Let S be the set of all real numbers and let "o" be the operation on S defined by:

$a \circ b = a \cdot a + a \cdot b - 1$, for all real numbers a and b.

If b is a real number, what is $1 \circ b$?

ANSWER:

$1 \circ b = b$. $1 \circ b = 1 \cdot 1 + 1 \cdot b - 1 = 1 + b - 1 = b$.

Is 1 an identity element for the operation "o"?

Explain.

ANSWER:

No. Although $1 \circ b = b$, for every real number b, it is not true that $b \circ 1 = b$, for every real number b. For example:

$2 \circ 1 = 2 \cdot 2 + 2 \cdot 1 - 1 = 4 + 2 - 1 = 5 \neq 2$.

---

5. Let S be a set. A binary operation on S is a function. Is it correct to say that the domain of the function is an ordered pair of elements of S? Explain.

ANSWER:

No. The domain is the set of all ordered pairs of elements of S, the set which we denote by $S \times S$.

If the binary operation on S is closed, then an element of the range of the function is in what set?

ANSWER:

S.

---

6. Let S be the set of positive real numbers; and let "o" be the binary operation on S defined as follows:

$$a \circ b = \frac{3 \cdot a \cdot b}{2a + 2b}, \quad \text{for all } a, b \text{ in } S.$$

Let $e = 2b$. Verify that $e \circ b = b \circ e = b$.

ANSWER:

$$e \circ b = \frac{3 \cdot e \cdot b}{2e + 2b} = \frac{3 \cdot 2b \cdot b}{2(2b) + 2b} = \frac{6 \cdot b \cdot b}{6 \cdot b} = b.$$

$$b \circ e = \frac{3 \cdot b \cdot e}{2b + 2e} = \frac{3 \cdot b \cdot 2b}{2b + 2(2b)} = \frac{6 \cdot b \cdot b}{6 \cdot b} = b.$$

Can we conclude that e is an identity element for the operation "o"? Explain.

ANSWER:

No. As defined, e depends upon the choice of the element b. In order for e to be an identity element it would have to be such that $e \circ b = b \circ e = b$ for every b in S. If $e = 2b$, the equation $e \circ b = b \circ e = b$ holds only for the particular b used in defining it. For example, if $b = 3$ and $e = 2 \cdot 3 = 6$, then

$e \circ 3 = 3 \circ e = 3$; but $e \circ 4 \neq 4$, since

$$6 \circ 4 = \frac{3 \cdot 6 \cdot 4}{2 \cdot 6 + 2 \cdot 4} = \frac{72}{20} = \frac{18}{5} \neq 4.$$

- -

III. ALGEBRAIC SYSTEMS

THEOREMS ON ADDITIVE AND MULTIPLICATIVE INVERSES

In the first part of this unit we will consider several theorems concerned with additive and multiplicative inverses of real numbers. You will of course already be familiar with the properties given in these theorems. You should pay particular attention however to the analogy that exists between theorems about addition and theorems about multiplication.

You will be asked to prove some of these theorems. Since it may become very tedious to show every time exactly how the associative and commutative properties are used in proofs, you may omit these properties throughout this unit except when they are specifically asked for. You need include parentheses only when they are required for clarity. However, in cases where you are asked to give the associative and commutative properties, you should show exactly how they are used and be very careful in the use of parentheses to indicate applications of the associative properties. In any event you should always give as reasons the other real number properties whenever they are used.

In your proofs you may use any theorem from Unit II and any theorem from this unit whose number precedes that of the theorem you are proving.

Theorem 3.1: If a and b are real numbers, $-(a + b) = (-a) + (-b)$.

What does $-(a - b)$ designate?

ANSWER:

The additive inverse of $(a + b)$.

- -

If the additive inverse of a real number is added to that number, the sum is ____.

- -

ANSWER:

0.

- -

We have already proved that the additive inverse of a real number is unique (Theorem 2.5). Therefore, if we can show that $((-a) + (-b)) + (a + b) = 0$ we can conclude that ____.

- -

ANSWER:

$(-a) + (-b) = -(a + b)$; i.e., $(-a) + (-b)$ is the additive inverse of $a + b$.

- -

Prove that $((-a) + (-b)) + (a + b) = 0$.

- -

PROOF:

1. $[(-a) + (-b)] + (a + b) = [(-a) + a] + [(-b) + b]$
2. $= 0 + 0$ $\quad A_{in}$
3. $= 0$ $\quad A_{id}$

[Note: In step 1, A_a and A_c are used; but as we previously stated you may use these properties without indicating how they are used. However, list other properties as reasons.]

- -

Theorem 3.1 is a statement about addition. There is an analogous theorem about multiplication. Theorem 3.1 states that the additive inverse of $(a + b)$ equals the additive inverse of a plus the additive inverse of b. The multiplicative theorem corresponding to Theorem 3.1 should state (in words) that ____.

ANSWER:

the multiplicative inverse of a times b equals the multiplicative inverse of a times the multiplicative inverse of b.

But this statement has meaning only if a and b are ____.

ANSWER:

non-zero real numbers.

Using symbols, the theorem can be stated as follows:

Theorem 3.2: If a and b are non-zero real numbers, ____ = ____.

ANSWER:

$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$

Prove Theorem 3.2 (using the proof of Theorem 3.1 as a guide, if necessary).

PROOF:

1. a^{-1} and b^{-1} exist since $a \neq 0$, $b \neq 0$ $\quad M_{in}$
2. $(a^{-1} \cdot b^{-1}) \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot (b^{-1} \cdot b)$
3. $\qquad = 1 \cdot 1$ $\quad M_{in}$
4. $\qquad = 1$ $\quad M_{id}$

This proves that $a^{-1} \cdot b^{-1}$ is a multiplicative inverse for $a \cdot b$. By Theorem 2.6, the multiplicative inverse is unique. Hence $a^{-1} \cdot b^{-1} = (a \cdot b)^{-1}$.

- -

THEOREM 3.3. $-0 = 0$.

State Theorem 3.3 in words.

- -

ANSWER:

The additive inverse of zero is zero.

- -

To show that the additive inverse of 0 is 0 we need only to observe that ____.

- -

ANSWER:

$0 + 0 = 0$

- -

$0 + 0 = 0$ is true by Property ____.

- -

ANSWER:

A_{id}.

- -

The multiplicative analogue of Theorem 3.3 is

THEOREM 3.4 (State the theorem using symbols.)

- -

ANSWER:

THEOREM 3.4: $1^{-1} = 1$.

- -

The proof of Theorem 3.4 is analogous to the proof of Theorem 3.3 and will not be given.

If a and b are real numbers, then $a + b = 0$ if and only if $a = -b$ and $b = -a$. This tells us that $-(-a) = -b = a$.

THEOREM 3.5: If a is a real number, then $-(-a) = a$.

State the multiplicative analogue of Theorem 3.5 which will be Theorem 3.6.

ANSWER:

THEOREM 3.6. If a is a non-zero real number, then $(a^{-1})^{-1} = a$.
[Did you forget to include the condition $a \neq 0$?]

The proof of Theorem 3.6 is analogous to the proof of Theorem 3.5; i.e., if a and b are non-zero real numbers, then $a \cdot b = 1$ if and only if $a = b^{-1}$ and $b = a^{-1}$, hence $(a^{-1})^{-1} = b^{-1} = a$. How do we know that if $a \neq 0$, then $b = a^{-1}$ is also non-zero?

ANSWER:

If $b = 0$ we would have $a \cdot b = 0$, by Theorem 2.3. But $a \cdot b = 1$ by M_{in}. Furthermore, $1 \neq 0$ by M_{id}. Hence $b \neq 0$.

The following theorem gives the sign laws for multiplication.

THEOREM 3.7: If a and b are real numbers,

(1) $a \cdot (-b) = -(a \cdot b)$

(2) $(-a) \cdot b = -(a \cdot b)$

(3) $(-a) \cdot (-b) = a \cdot b$

Proof: (1) To show $a(-b) = -(ab)$ we must prove that ____ $= 0$.

ANSWER:

$a(-b) + ab$.

Complete the proof of (1)

ANSWER:

1. $a(-b) + ab = a(-b + b)$	1. D
2. $\qquad = a \cdot 0$	2. A_{in}
3. $\qquad = 0$	3. Theorem 2.3
4. $a(-b) = -(ab)$	4. Definition of inverse, Theorem 2.5

You may be tempted to prove (1) by substituting $(-1) \cdot b$ in place of $-b$. Note, however, that $-b$ is not defined to be $(-1) \cdot b$. In fact the equality $(-1) \cdot b = -b$ is a special example of (2) of Theorem 3.7. If we take $a = 1$ in (2) we get $(-1) \cdot b = -(1 \cdot b) = -b$. If you used $(-1) \cdot b = -b$ in your proof of (1) it is not correct.

Prove (2) using (1) and M_c.

ANSWER:

1. $(-a) \cdot b = b \cdot (-a)$	M_c
2. $\qquad = -(b \cdot a)$	Part (1)
3. $\qquad = -(a \cdot b)$	M_c
4. $(-a) \cdot b = -(a \cdot b)$	

See if you can find an error in the following proof of (3).

PROOF:

1. $(-a) \cdot (-b) = -[(-a) \cdot b]$	Part (1)
2. $\qquad = -[-(a \cdot b)]$	Part (2)

3. $= a \cdot b$ M_a

ANSWER:

The reason in step 3 is not correct. The correct reason is Theorem 3.5.

The proof given is correct if we change the reason in step 3 from M_a to Theorem 3.5. State the multiplicative analogue of Theorem 3.7.

ANSWER:

Theorem 3.7 involves both addition and multiplication, so it does not have a "multiplicative analogue".

Is Theorem 3.7 also valid for the arithmetic modulo 3, I/3? If not, why not?

ANSWER:

Yes. All the field postulates are valid for I/3, and only these have been used in our proof.

Is Theorem 3.7 also valid for I/12? If not, why not?

ANSWER:

Yes. All the field postulates except M_{in} are valid for I/12. The proof of Theorem 3.7 in no way depends upon Property M_{in}.

It is worth pointing out here an objection to learning the sign laws in Theorem 3.7 as "positive times negative equals negative," "negative times positive equals negative," etc. We will see later that the notions of positive and negative depend very strongly on the ordering that we have in the set of real numbers. However the use of the minus sign in Theorem 3.7 is to denote the additive inverse of a real number, a notion which is not dependent upon the ordering. In fact, Theorem 3.7 is valid in the modular arithmetics (e.g., I/3, I/4, I/12) and in these systems the notions of positive and negative have no meaning. It is therefore incorrect to think of Part (3) of Theorem 3.7 as saying: "The product of two negative numbers is positive."

The following theorem also involves both addition and multiplication properties.

THEOREM 3.8: If b is a non-zero real number, $(-b)^{-1} = -(b^{-1})$.

In other words, the order in which we take the additive and multiplicative inverses of b does not affect the result.

There are several ways of proving Theorem 3.8. There is one way of looking at the theorem, however, which leads to a very simple proof. The theorem says that $-(b^{-1})$ is the ____ of $-b$.

- -

ANSWER:
multiplicative inverse

- -

Therefore we must show that ____ $= 1$.

- -

ANSWER:
$-(b^{-1}) \cdot -b$

- -

Prove that $-(b^{-1}) \cdot -b = 1$.

- -

Did you use Theorem 3.7 Part (3) in your proof? If so, check your proof with the one given below.

- -

PROOF:

$-(b^{-1}) \cdot -b$	$= b^{-1} \cdot b$	Theorem 3.7 Part (3)
	$= 1$	M_{in}

- -

We could have interpreted the theorem as saying that $(-b)^{-1}$ is the additive inverse of b^{-1}. Then we could prove this by showing that $(-b)^{-1} + b^{-1} = 0$. To do this we observe that

$(-b) \cdot [(-b)^{-1} + b^{-1}]$	$= (-b) \cdot (-b)^{-1} + (-b) \cdot b^{-1}$	Property D
	$= 1 + (-b) \cdot b^{-1}$	M_{in}
	$= 1 + [-(b \cdot b^{-1})]$	Theorem 3.7 part (2)
	$= 1 + [-1]$	M_{in}
	$= 0$	A_{in}
Since $-b \neq 0$, we conclude $(-b)^{-1} + b^{-1} = 0$		Theorem 2.4

Is Theorem 3.8 valid for I/3? If not, why not?

- -

ANSWER:

Yes

- -

Is Theorem 3.8 valid for I/12? If not, why not?

- -

ANSWER:

No. Property M_{in} fails for I/12. Theorem 3.8 requires that b^{-1} exist for each non-zero b. This is not true in I/12.

The following theorem states that multiplication is distributive over subtraction. It is similar to Property D, one of our postulates. You should expect to have to use Property D in the proof.

THEOREM 3.9: If a, b, and c are real numbers, then $a \cdot (b - c) = a \cdot b - a \cdot c$.

How can we rewrite $a \cdot (b - c)$ in a form to which we can apply Property D?

ANSWER:

$a \cdot (b - c) = a \cdot (b + [-c])$, using definition of subtraction.

Complete the proof of Theorem 3.9.

Have you used Theorem 3.7? If not, check your proof before proceeding.

PROOF:

1.	$a(b - c) = a(b + (-c))$	Definition of subtraction
2.	$= (ab) + (a(-c))$	D
3.	$= (ab) + (-(ac))$	Theorem 3.7
4.	$= (ab) = (ac)$	Definition of subtraction

The next theorem gives the sign laws for division. You should expect to use Theorem 3.7 in your proof.

THEOREM 3.10: If a and b are real numbers and $b \neq 0$, then

(1) $(-a) \div b = -(a \div b)$, or $\frac{-a}{b} = -\frac{a}{b}$

(2) $a \div (-b) = -(a \div b)$, or $\frac{a}{-b} = -\frac{a}{b}$

(3) $(-a) \div (-b) = (a \div b)$, or $\frac{-a}{-b} = \frac{a}{b}$

Complete the proof of part (1).

1.	$(-a) \div b = -a \cdot (b^{-1})$	Definition of division

- -

ANSWER:

1.	$(-a) \div b = (-a) \cdot (b^{-1})$	Definition of division
2.	$= -[a \cdot (b^{-1})]$	Theorem 3.7
3.	$= -(a \div b)$	Definition of division

- -

Prove part (2).

- -

Have you used Theorem 3.8 in the proof of part (2)? If not, check your proof before proceeding.

- -

Proof of part (2):

1.	$a \div (-b) = a \cdot ((-b)^{-1})$	Definition of division
2.	$= a \cdot (-(b^{-1}))$	Theorem 3.8
3.	$= -(a \cdot b^{-1})$	Theorem 3.7
4.	$= -(a \div b)$	Definition of division

- -

Prove part (3) without using part (1) or part (2).

- -

ANSWER:

1.	$(-a) \div (-b) = (-a) \cdot ((-b)^{-1})$	Definition of division
2.	$= (-a) \cdot (-(b^{-1}))$	Theorem 3.8
3.	$= a \cdot (b^{-1})$	Theorem 3.7
4.	$= a \div b$	Definition of division

- -

Prove part (3) using part (1) and part (2).

- -

ANSWER:

1. $(-a) + (-b) = -(a + (-b))$ Part (1)
2. $= -(-(a + b))$ Part (2)
3. $= a + b$ Theorem 3.5

- -

MATRICES

In this section we give some further examples of mathematical systems having properties in common with the real number system.

A matrix is a rectangular array of real numbers, for example: $\begin{bmatrix} 2 & 3 \\ 7 & 4 \end{bmatrix}$. The real numbers are arranged in rows and columns. The given example has two rows and two columns. Be careful to note that we are not concerned here with determinants, we are only concerned with the matrices as arrays of numbers. In the first part of this section we will restrict our attention to two-row, two-column matrices. Later we will consider other types of matrices.

Matrices are equal if all corresponding elements are equal. Thus $\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ means $a = e$, $b = f$, $c = g$, and $d = h$.

We wish to define two binary operations, addition and multiplication, on the set of all two-row, two-column matrices.

DEFINITION OF "+": $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} (a + q) & (b + r) \\ (c + s) & (d + t) \end{bmatrix}$

For example: $\begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 3 \\ 1 & -6 \end{bmatrix} = \begin{bmatrix} (2 + 5) & (1 + 3) \\ (7 + 1) & (4 + (-6)) \end{bmatrix} = \begin{bmatrix} 7 & 4 \\ 8 & -2 \end{bmatrix}$

$$\begin{bmatrix} 3 & -2 \\ 4 & 6 \end{bmatrix} + \begin{bmatrix} 4 & 1 \\ 7 & -8 \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

- -

ANSWER:

$$\begin{bmatrix} 7 & -1 \\ 11 & -2 \end{bmatrix}$$

$\begin{bmatrix} 3 & -2 \\ 4 & 6 \end{bmatrix} + \begin{bmatrix} ? \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ 4 & 6 \end{bmatrix}$

ANSWER:

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

$\begin{bmatrix} ? \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

ANSWER:

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

The matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the ____ for matrix addition.

ANSWER:

identity element

$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} ? \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

ANSWER:

$\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$

Also, $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Therefore the additive inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is ____.

ANSWER:

$$\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$$

- -

Consider the following proof:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} (a+q) & (b+r) \\ (c+s) & (d+t) \end{bmatrix} \quad \text{Defintion of +}$$

$$= \begin{bmatrix} (q+a) & (r+b) \\ (s+c) & (t+d) \end{bmatrix} \quad A_c \text{ for real numbers}$$

$$= \begin{bmatrix} q & r \\ s & t \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{Definition of +}$$

and thus

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} q & r \\ s & t \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We conclude that matrix addition is ____.

- -

ANSWER:

commutative. (or, a commutative operation)

- -

In a similar manner, prove that matrix addition is an associative operation. In other words, prove:

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix}\right)$$

Indicate exactly how A_a for real numbers is used in your proof.

- -

ANSWER:

$$\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix}\right) + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} (a+e) & (b+f) \\ (c+g) & (d+h) \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix}$$

Definition of +

$$= \begin{bmatrix} (a+e)+q & (b+f)+r \\ (c+g)+s & (d+h)+t \end{bmatrix}$$

Definition of +

$$= \begin{bmatrix} a + (e + q) & b + (f + r) \\ c + (g + s) & d + (h + t) \end{bmatrix}$$

A_a for real numbers

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} (e + q) & (f + r) \\ (g + s) & (h + t) \end{bmatrix}$$

Definition of +

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix} \right)$$

Definition of +

$$\therefore \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} q & r \\ s & t \end{bmatrix} \right)$$

Having observed that the operation is closed and has the above properties we can conclude that 2 × 2 matrices from a(n) ____ under matrix addition.

ANSWER:
commutative group.

DEFINITION OF ".": $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} q & r \\ s & t \end{bmatrix} = \begin{bmatrix} (aq + bs) & (ar + bt) \\ (cq + ds) & (cr + dt) \end{bmatrix}$

Note: An element in 1st row and 2nd column (upper right corner) of the product is obtained by adding the products obtained by multiplying the elements of the 1st row of the first matrix by the corresponding elements of the 2nd column of the second matrix. The other elements are similarly obtained. For example, the element in the 2nd row and 1st column of the product is obtained by adding the products obtained by multiplying the elements of the ____ of the first matrix by the corresponding elements of the ____ of the second matrix.

ANSWER:

2nd row

1st column

- -

$$\begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 1 & -6 \end{bmatrix} = \begin{bmatrix} (2 \cdot 5 + 1 \cdot 1) & (2 \cdot 3 + 1 \cdot (-6)) \\ (7 \cdot \underset{\uparrow}{\_} + 4 \cdot \underset{\uparrow}{\_}) & (\underset{\uparrow}{\_} \cdot 3 + \underset{\uparrow}{\_} \cdot (-6)) \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

- -

ANSWER:

$$\begin{bmatrix} (2 \cdot 5 + 1 \cdot 1) & (2 \cdot 3 + 1 \cdot (-6)) \\ (7 \cdot 5 + 4 \cdot 1) & (7 \cdot 3 + 4 \cdot (-6)) \end{bmatrix} = \begin{bmatrix} 11 & 0 \\ 39 & -3 \end{bmatrix}$$

- -

$$\begin{bmatrix} 2 & -5 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 7 & 2 \\ 4 & -2 \end{bmatrix} =$$

- -

ANSWER:

$$\begin{bmatrix} -6 & 24 \\ 25 & 2 \end{bmatrix}$$

- -

Reverse the order of the above pair of matrices and compute their product. Is matrix multiplication commutative?

- -

ANSWER:

$$\begin{bmatrix} 7 & 2 \\ 4 & -4 \end{bmatrix} \cdot \begin{bmatrix} 2 & -5 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 20 & -33 \\ -4 & -24 \end{bmatrix}$$

$$\begin{bmatrix} 2 & -5 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 7 & 2 \\ 4 & -4 \end{bmatrix} = \begin{bmatrix} -6 & 24 \\ 25 & 2 \end{bmatrix}$$

Matrix multiplication is not commutative.

- -

If $\begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix}$

then: $3a + 7c = 3$

$3b + 7d = 7$

(Determine the two remaining equations.)

ANSWER:

$a + 4c = 1$

$b + 4d = 4$

From this we obtain a pair of equations in a and c and another pair of equations in b and d.

$3a + 7c = 3$

$a + 4c = 1$

Solve this system of equations for a and c.

ANSWER:

$3a + 7c = 3$

$3a + 12c = 3$

$\therefore 5c = 0 \quad a = 1, \quad c = 0$

Similarly, we may determine b = ____, d = ____.

ANSWER:

$b = 0$, $d = 1$ from $3b + 7d = 7$

$b + 4d = 4$

Therefore, $\begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} ? \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix}$

ANSWER:

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

- -

Is the following statement true for all real numbers a, b, c, and d?

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

- -

ANSWER:

Yes.

- -

When we defined the term "identity element", we required that if e is an identity element for an operation "$\cdot$" on a set S, $e \cdot a = a \cdot e = a$ for each a in the set S. All of the systems we have previously considered have possessed the commutative property; so if $e \cdot a = a$, we knew $a \cdot e = a$.

But matrix multiplication is not commutative. Therefore we must also test the equation ____ to see if the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is an identity element for matrix multiplication.

ANSWER:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

- -

Is the above equation true for all real numbers a, b, c, and d?

- -

ANSWER:

Yes.

- -

Find the four real number equations that result from the following statement:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

ANSWER:

$aw + by = 1$

$ax + bz = 0$

$cw + dy = 0$

$cx + dz = 1$

Solve the above equations for w, x, y, and z in terms of a, b, c, and d. You may assume that $a \cdot d - b \cdot c \neq 0$.

ANSWER:

$$w = \frac{d}{ad - bc} \qquad y = \frac{-c}{ad - bc}$$

$$x = \frac{-b}{ad - bc} \qquad z = \frac{a}{ad - bc} \qquad \text{if } ad - bc \neq 0.$$

The above method for finding the multiplicative inverse of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ fails in case $ad - bc = 0$. In fact, it can be shown, although we will not do so, that if $ad - bc = 0$ then the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ does not have an inverse under multiplication.

If ____ $\neq 0$, $\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$ is the ____ of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

ANSWER:

ad - bc; multiplicative inverse

What is the multiplicative inverse of $\begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix}$?

Check your answer by multiplication (check the product in both orders).

ANSWER:

$$\begin{bmatrix} 4/5 & -7/5 \\ -1/5 & 3/5 \end{bmatrix}$$

CHECK:

$$\begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 4/5 & -7/5 \\ -1/5 & 3/5 \end{bmatrix} = \begin{bmatrix} 3(4/5) + 7(-1/5) & 3(-7/5) + 7(3/5) \\ 1(4/5) + 4(-1/5) & 1(-7/5) + 4(3/5) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Also, $\begin{bmatrix} 4/5 & -7/5 \\ -1/5 & 3/5 \end{bmatrix} \cdot \begin{bmatrix} 3 & 7 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Does $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ always have an inverse under matrix multiplication if $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$?

ANSWER:

No. Any matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for which $ad - bc = 0$ fails to have a multiplicative inverse; e.g., $\begin{bmatrix} 2 & 4 \\ -1 & -2 \end{bmatrix}$.

Thus the inverse property does not hold for 2 × 2 matrices under multiplication.

We have not yet considered whether matrix multiplication is associative. The detailed proof is quite long and therefore we will only consider a part of it.

We will calculate the term in the first row and first column of the final products obtained by the two associations. After showing that these elements are equal we will assume the same thing could be done for the other elements. The notation will be changed slightly in order to keep track of terms more easily.

Fill in each of the blanks; be sure to include all of the necessary parentheses.

$$\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}\right) \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = \begin{bmatrix} \text{(Omit the} \\ \text{second row)} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$$

[Note: The subscripts appearing on the letters a, b, c, above indicate the row and column in which the element lies; e.g., a_{12} lies in row 1 and column 2.]

ANSWER:

$$\begin{bmatrix} a_{11}\,b_{11} + a_{12}\,b_{21} & a_{11}\,b_{12} + a_{12}\,b_{22} \\ \text{(Omit the second row)} & \end{bmatrix}$$

$$\begin{bmatrix} a_{11}\,b_{11} + a_{12}\,b_{21} & a_{11}\,b_{12} + a_{12}\,b_{22} \\ \text{(omit)} & \text{(omit)} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} =$$

$$\begin{bmatrix} \\ \text{(Omit the second row and the second column)} \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} (a_{11}\,b_{11} + a_{12}\,b_{21})c_{11} + (a_{11}\,b_{12} + a_{12}\,b_{22})c_{21} & \text{(Omit)} \\ \text{(Omit)} & \text{(Omit)} \end{bmatrix}$$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \left(\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \cdot \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}\right) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} \text{(Omit the sec-} \\ \text{ond column)} \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} b_{11}\ c_{11} + b_{12}\ c_{21} & \text{(Omit)} \\ b_{21}\ c_{11} + b_{22}\ c_{21} & \text{(Omit)} \end{bmatrix}$$

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11}\ c_{11} + b_{12}\ c_{21} & \text{(Omit)} \\ b_{21}\ c_{11} + b_{22}\ c_{21} & \text{(Omit)} \end{bmatrix} = \begin{bmatrix} \text{(Omit the second} \\ \text{row and the sec-} \\ \text{ond column)} \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} a_{11}\ (b_{11}\ c_{11} + b_{12}\ c_{21}) + a_{12}\ (b_{21}\ c_{11} + b_{22}\ c_{21}) & \text{(Omit)} \\ \text{(Omit)} & \text{(Omit)} \end{bmatrix}$$

It is straightforward to check that:

$(a_{11}\ b_{11} + a_{12}\ b_{21})\ c_{11} + (a_{11}\ b_{12} + a_{12}\ b_{22})\ c_{21} = a_{11}\ (b_{11}\ c_{11} + b_{12}\ c_{21}) + a_{12}\ (b_{21}\ c_{11} + b_{22}\ c_{21})$.

This completes the proof.

In summary, we see that the system of two-row, two-column matrices with matrix addition and multiplication satisfies all the field postulates except for M_c and M_{in}. Any theorem that we have proved about real numbers and whose proof did not make use of Properties M_c and M_{in} is valid for this sytem of matrices. In particular, all the theorems which are concerned only with the addition operation are valid.

We illustrate with an example one theorem which is not valid for the system of matrices. Let A and B be matrices defined as follows:

$$A = \begin{bmatrix} 1 & -1 \\ -2 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 \\ 3 & 1 \end{bmatrix}$$

Then A and B are non-zero matrices but $A \cdot B$ is the zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. This example shows that Theorem 2.4 is not valid for matrices.

We turn now to more general types of matrices. We will say that a matrix is an $m \times n$ matrix if it has m rows and n columns. The matrices we have been discussing thus far are 2×2 matrices. We will often use capital letters to denote matrices and lower case letters with double subscripts to denote elements of the matrix. Thus a_{ij} will denote the element in the i^{th} row and j^{th} column of a matrix.

DEFINITION 3.1: Suppose A and B are $m \times n$ matrices, i.e., A and B have the same number of rows and the same number of columns. If a_{ij} denotes the element in the i^{th} row and j^{th} column of A, and b_{ij} denotes the element in the i^{th} row and j^{th} column of B, then $A + B$ is defined to be that $m \times n$ matrix such that the element in the i^{th} row and j^{th} column is $a_{ij} + b_{ij}$, for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Note that the above definition agrees with the definition we have already adopted for 2×2 matrices. Note also that $A + B$ is not defined unless A and B have the same number of rows and same number of columns.

Find the sum:

$$\begin{bmatrix} 3 & 1 & 2 \\ 4 & 2 & 5 \end{bmatrix} + \begin{bmatrix} -1 & 4 & -3 \\ 2 & 0 & 4 \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 2 & 5 & -1 \\ 6 & 2 & 9 \end{bmatrix}$$

Find the sum:

$$\begin{bmatrix} 1 \\ 0 \\ 4 \end{bmatrix} + \begin{bmatrix} 2 \\ -1 \\ -2 \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 3 \\ -1 \\ 2 \end{bmatrix}$$

DEFINITION 3.2: If A is an $n \times m$ matrix and B is an $m \times p$ matrix, then $A \cdot B$ is the $n \times p$ matrix obtained by the following procedure: the element in the i^{th} row and j^{th} column of $A \cdot B$ is equal to the sum of the products of corresponding elements of the i^{th} row of A and the j^{th} column of B.

Be sure to note that in the above definition the second matrix, B, must have the same number of rows as the first matrix, A, has columns. The product $A \cdot B$ then has as many rows as A and as many columns as B.

Find the product of the following two matrices:

$$\begin{bmatrix} 3 & 1 & 2 \\ 4 & 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 1 & -4 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} & & \\ & ? & \\ & & \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 3 \cdot 2 + 1 \cdot 1 + 2 \cdot (-1) & 3 \cdot 3 + 1 \cdot (-4) + 2 \cdot 2 \\ 4 \cdot 2 + 2 \cdot 1 + 5 \cdot (-1) & 4 \cdot 3 + 2 \cdot (-4) + 5 \cdot 2 \end{bmatrix} = \begin{bmatrix} 5 & 9 \\ 5 & 14 \end{bmatrix}$$

Find the product:

$$\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 4 \\ 5 & 3 & -4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -2 \\ 4 \end{bmatrix} = \begin{bmatrix} \\ ? \\ \\ \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 1 \cdot 1 + 3 \cdot (-2) + 2 \cdot 4 \\ 2 \cdot 1 + 1 \cdot (-2) + 4 \cdot 4 \\ 5 \cdot 1 + 3 \cdot (-2) + (-4) \cdot 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 16 \\ -17 \end{bmatrix}$$

Find the product:

$$\begin{bmatrix} 3 & 1 & 2 \\ 4 & 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 2 & 3 \\ 1 & -4 \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

The product cannot be obtained since the number of rows in the second matrix is not equal to the number of columns in the first matrix.

Find the product:

$$\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 4 \\ 5 & 3 & -4 \end{bmatrix} \cdot \begin{bmatrix} 3 & -2 & 4 \\ 1 & 6 & 3 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 10 & 18 & 17 \\ 15 & 6 & 19 \\ 10 & 4 & 21 \end{bmatrix}$$

If A is a 5 × 3 matrix and B is a 3 × 7 matrix, then A · B is a ____ matrix.

ANSWER:

5 × 7

If A is a 5 × 1 matrix and B is a 1 × 5 matrix, then A · B is a ____ matrix and B × A is a ____ matrix.

ANSWER:

5 × 5

1 × 1

Observe that the product definition does not allow us to choose arbitrarily two matrices and determine the matrix to which this "operation" would assign them. Therefore this definition fails to define an operation over the set of all matrices. Matrix multiplication can be shown to be associative whenever it is defined. Thus if A is an $n \times m$ matrix, B is an $m \times p$ matrix, and C is a $p \times q$ matrix, then all of the products indicated in the expressions $(A \cdot B) \cdot C$ and $A \cdot (B \cdot C)$ are defined and $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. Each of these expressions denotes an $n \times q$ matrix.

For any given positive integer n, addition and multiplication are closed operations on the set of all $n \times n$ matrices. It can be shown, just as we indicated previously for the case $n = 2$, that for the system of $n \times n$ matrices all the field postulates are valid except for M_c and M_{in}. In particular the multiplicative identity for this system is the matrix whose main diagonal entries are all equal to 1 and all of whose off-diagonal elements are equal to 0. These matrices are shown below for $n = 3, 4, 5$.

$$n = 3 \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad n = 4 \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad n = 5 \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

We call these matrices multiplicative identity matrices. More generally, if I denotes the $n \times n$ multiplicative identity matrix, then $I \cdot A = A$ for any matrix A with n rows (and any number of columns) and $A \cdot I = A$ for any matrix A with n columns (and any number of rows).

Matrices have been applied with great success to the problem of solving systems of linear equations.

For the first illustration of such an application we will consider the following system of equations:

$$2x + 3y = 1$$
$$4x + y = 5$$

Find the product of the following two matrices:

$$\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 2x + 3y \\ 4x + y \end{bmatrix}$$

The two elements in the product matrix are the expressions on the left sides of the two equations. Since two matrices are equal if their corresponding elements are equal we can rewrite the given pair of equations in the following matrix form:

$$\begin{bmatrix} ? \end{bmatrix} \cdot \begin{bmatrix} ? \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \end{bmatrix}$$

The matrix $\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$ has the coefficients from the equation system as its entries and is usually referred to as the coefficient matrix. Construct the matrix equation which is equivalent to the following system of equations:

$4x + 7y = 11$

$2x + 3y = 5$

ANSWER:

$$\begin{bmatrix} 4 & 7 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix}$$

Each of the above matrix equations is of the form $A \cdot X = B$ where A, X, and B are matrices. When we solve a real number equation of the form $a \cdot x = b$ and $a \neq 0$, we "divide both sides of the equation by a" and arrive at the solution $x = b/a$. But division is defined in terms of multiplication and depends on the existence of the multiplicative inverse for its meaning. Thus a more basic way of arriving at the solution of the equation $a \cdot x = b$ is to multiply both sides of the equation by a^{-1} thus obtaining $x = a^{-1} \cdot b$. A similar approach can be used to solve the matrix equation $A \cdot X = B$. If A^{-1} exists we can multiply both sides of the equation by it and arrive at the equation $A^{-1} \cdot (A \cdot X) = A^{-1} \cdot B$. (The order of the multiplication is important since M_c does not hold for matrix multiplication.)

But $A^{-1} \cdot (A \cdot X) =$ ____.

- -

ANSWER:

X; $A^{-1} \cdot (A \cdot X) = (A^{-1} \cdot A) \cdot X = I \cdot X = X$. Remember that matrix multiplication is associative.

- -

Thus $X =$ ____.

- -

ANSWER:

$A^{-1} \cdot B$.

- -

The solution of the equation $\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 5 \end{bmatrix}$ can be obtained by first finding the inverse of $\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$, if it exists. Recall that the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ has as its inverse the matrix $\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$, provided $ad - bc \neq 0$.

Find the inverse of $\begin{bmatrix} 2 & 3 \\ 4 & 1 \end{bmatrix}$.

ANSWER:

$$\begin{bmatrix} \frac{1}{-10} & \frac{-3}{-10} \\ \frac{-4}{-10} & \frac{2}{-10} \end{bmatrix} = \begin{bmatrix} \frac{-1}{10} & \frac{3}{10} \\ \frac{4}{10} & \frac{-2}{10} \end{bmatrix}$$

Therefore $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix} \cdot \begin{bmatrix} ? \end{bmatrix}$

ANSWER:

$$\begin{bmatrix} \frac{-1}{10} & \frac{3}{10} \\ \frac{4}{10} & \frac{-2}{10} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 5 \end{bmatrix}$$

From the above we obtain $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ? \end{bmatrix}$

ANSWER:

$$\begin{bmatrix} \frac{14}{10} \\ \frac{-6}{10} \end{bmatrix}$$

Since $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \frac{14}{10} \\ \frac{-6}{10} \end{bmatrix}$ is the solution of the matrix equation, we know $x =$ _____, $y =$ ____ is the solution of the original system of equations.

ANSWER:

$x = 14/10$ or $7/5$

$y = -6/10$ or $-3/5$

- -

By the given method find the solution of the matrix equation $\begin{bmatrix} 4 & 7 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix}$ and the solution of the associated system of equations.

- -

ANSWER:

The inverse of $\begin{bmatrix} 4 & 7 \\ 2 & 3 \end{bmatrix}$ is $\begin{bmatrix} \frac{3}{-2} & \frac{7}{2} \\ 1 & -2 \end{bmatrix}$

Therefore $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \frac{-3}{2} & \frac{7}{2} \\ 1 & -2 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 5 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Thus $x = 1$, $y = 1$ is the solution of the system of equations.

- -

Solve the following system of equations by the matrix method:

$-4x + 2y = 3$

$-6x + 4y = 1$

- -

ANSWER:

$$\begin{bmatrix} -4 & 2 \\ -6 & 4 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{4}{-4} & \frac{-2}{-4} \\ \frac{6}{-4} & \frac{-4}{-4} \end{bmatrix} \quad \therefore \quad \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & \frac{1}{2} \\ \frac{-3}{2} & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{-5}{2} \\ \frac{-7}{2} \end{bmatrix}$$

$x = \frac{-5}{2}$, $y = \frac{-7}{2}$

- -

We should perhaps point out that matrices play a fundamental role in vector geometry, the importance of which is such that a course in vectors and matrices is now standard in college for practically all mathematics majors and for many students who major in such fields as physics, statistics, economics, and many of the social sciences.

THEOREMS ON FRACTIONS

In this section we will present several more theorems on real numbers. The results contained in these theorems are the familiar rules for addition, subtraction, multiplication, and division of fractions.

If a and b are real numbers, $b \neq 0$, then we denote by $a \div b$ or by a/b the quotient a divided by b. We have:

$$a \div b = a/b = a \cdot b^{-1} = b^{-1} \cdot a.$$

Suppose n is a positive integer greater than 1 and that A and B are $n \times n$ matrices. Since M_{in} is not valid for the system of $n \times n$ matrices, $A \div B$ may not be defined even if B is not the zero matrix, because B may not have an inverse under multiplication. Even if B^{-1} does exist there is still a problem in writing:

$$A \div B = A/B = A \cdot B^{-1} = B^{-1} \cdot A.$$

What is the problem?

ANSWER:

M_c is also not valid for the system of $n \times n$ matrices. Hence we might have $A \cdot B^{-1} = B^{-1} \cdot A$.

It should be clear from the preceding discussion that we cannot expect that the rules for operating with quotients of real numbers should be valid for matrices.

For real numbers, the familiar rule for adding fractions is the following:

THEOREM 3.11: If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then $a/b + c/d = \frac{a \cdot d + c \cdot b}{b \cdot d}$

Prove this theorem by starting with the right hand expression and changing it to the left hand expression. Give reasons for your steps, except for the associative and commutative properties.

- -

Did you use Theorem 3.2 to convert $(b \cdot d)^{-1}$ to $b^{-1} \cdot d^{-1}$?

Did you use Property D? If not, check your proof before proceeding.

- -

ANSWER:

1. $\frac{a \cdot d + c \cdot b}{b \cdot d} = (a \cdot d + c \cdot b) \cdot (b \cdot d)^{-1}$
2. $= (a \cdot d + c \cdot b) \cdot (b^{-1} \cdot d^{-1})$
3. $= a \cdot d \cdot b^{-1} \cdot d^{-1} + c \cdot b \cdot b^{-1} \cdot d^{-1}$
4. $= (a \cdot b^{-1}) \cdot (d \cdot d^{-1}) + (c \cdot d^{-1}) \cdot (b \cdot b^{-1})$
5. $= (a \cdot b^{-1}) \cdot 1 + (c \cdot d^{-1}) \cdot 1$
6. $= a \cdot b^{-1} + c \cdot d^{-1}$
7. $= a/b + c/d$

1. Definition of division
2. Theorem 3.2
3. D
4.
5. M_{in}
6. M_{id}
7. Definition of division

- -

THEOREM 3.12: If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then

$a/b - c/d = \frac{a \cdot d - c \cdot b}{b \cdot d}$

The proof given above for Theorem 3.11 will also serve as a proof for Theorem 3.12 if we change in each step the "plus" sign to a "minus" sign. However we must also change the reason for step 3. Instead of Property D we should list ____ as reason.

- -

ANSWER:

Theorem 3.9 (Actually Theorem 3.9 and M_c, but we have agreed to use M_c without listing it as a reason.)

- -

THEOREM 3.13: If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then

$a/b \cdot c/d = ac/bd$.

We can rewrite as follows:

$\frac{a \cdot c}{b \cdot d} = (ac) \cdot (bd)^{-1}$, $a/b = a \cdot b^{-1}$, $c/d = c \cdot d^{-1}$.

Prove Theorem 3.13.

- -

ANSWER:

1. $a/b \cdot c/d = (a \cdot b^{-1}) \cdot (c \cdot d^{-1})$ Definition of division
2. $= (a \cdot c) \cdot (b^{-1} \cdot d^{-1})$
3. $= (a \cdot c) \cdot (b \cdot d)^{-1}$ Theorem 3.2
4. $= ac/bd$ Definition of division

- -

THEOREM 3.14: If a, b, c, and d are real numbers with $b \neq 0$, $c \neq 0$, and $d \neq 0$, then

$a/c \div c/d = \frac{a \cdot d}{b \cdot c}$

By Theorem 3.13, $d/c \cdot c/d = dc/cd = (cd)\,(cd)^{-1} = 1$. This proves that $c/d \neq 0$ (by Theorem 2.4) and that $(c/d)^{-1} =$ ____.

- -

ANSWER:

d/c.

- -

Using the fact that $c/d \neq 0$ and $(c/d)^{-1} = d/c$, prove Theorem 3.14.

1. $c/d \neq 0$ and $(c/d)^{-1} = d/c$ Proved above

(Complete the proof)

- -

ANSWER:

1. $c/d \neq 0$ and $(c/d)^{-1} = d/c$ Proved above
2. $a/b \div c/d = a/b \cdot (c/d)^{-1}$ Definition of division
3. $\quad = a/b \cdot d/c$ Step 1
4. $\quad = ad/bc$ Theorem 3.13

- -

Theorem 3.14 is the familiar rule for dividing fractions, "invert the denominator and multiply."

Suppose we try to write down a theorem for 2×2 matrices similar to Theorem 3.11. We might try the following statement.

If A, B, C, and D are 2×2 matrices and if B^{-1} and D^{-1} exist, then

$$A \cdot B^{-1} + C \cdot D^{-1} = (A \cdot D + C \cdot B) \cdot (B \cdot D)^{-1}.$$

What mistakes can you find in the following "proof" of this statement?

PROOF:

1. $(A \cdot D + C \cdot B) \cdot (B \cdot D)^{-1} = (A \cdot D + C \cdot B) \cdot (B^{-1} \cdot D^{-1})$
2. $\quad = A \cdot D \cdot B^{-1} \cdot D^{-1} + C \cdot B \cdot B^{-1} \cdot D^{-1}$
3. $\quad = (A \cdot B^{-1}) \cdot (D \cdot D^{-1}) + C \cdot (B \cdot B^{-1}) \cdot D^{-1}$

4. $= (A \cdot B^{-1}) \cdot I + C \cdot I \cdot D^{-1}$

5. $= A \cdot B^{-1} + C \cdot D^{-1}$

ANSWER:

There is a mistake in step 1. We do not know that $(BD)^{-1} = B^{-1} \cdot D^{-1}$. The proof of Theorem 3.2 makes use of M_c, which is not valid for 2×2 matrices. Step 2 is an application of Property D (and M_a) and is valid. Step 3 is not valid because Property M_c is used. Steps 4 and 5 are valid.

Actually the statement for which we have given an incorrect proof is not true.

THEOREM 3.15: If a, b, c, and d are real numbers with $b \neq 0$ and $d \neq 0$, then $a/b = c/d$ if and only if $a \cdot d = c \cdot b$.

A statement, like that given above, using the phrase "if and only if" is equivalent to a theorem in the "If ... then ..." form and its converse. Thus there are two parts in the proof of Theorem 3.15. In the "if" part of the proof we prove that $a/b = c/d$ if $a \cdot d = c \cdot b$ where ____ is the hypothesis and ____ is the conclusion.

ANSWER:

$a \cdot d = c \cdot b$

$a/b = c/d$

In the "only if" part of the theorem the hypothesis is ____ and the conclusion is ____.

ANSWER:

$a/b = c/d$

$a \cdot d = c \cdot b$

Consider the following proof:

1. $a \cdot d = c \cdot b$
2. $b \neq 0$, $d \neq 0$, hence b^{-1} and d^{-1} exist
3. $(a \cdot d) \cdot (b^{-1} \cdot d^{-1}) = (c \cdot b) \cdot (b^{-1} \cdot d^{-1})$
4. $(a \cdot b^{-1}) \cdot (d \cdot d^{-1}) = (c \cdot d^{-1}) \cdot (b \cdot b^{-1})$
5. $(a \cdot b^{-1}) \cdot 1 = (c \cdot d^{-1}) \cdot 1$
6. $a \cdot b^{-1} = c \cdot d^{-1}$
7. $a/b = c/d$

1.
2. Hypothesis and M_{in}
3.
4. M_a and M_c
5. M_{in}
6. M_{id}
7. Definition of division

This proves which part of Theorem 3.15, the "if" part or the "only if" part?

ANSWER:

The "if" part. (Note that the reasoning proceeds from the hypothesis $a \cdot d = c \cdot b$ to the conclusion $a/b = c/d$.)

The steps in the proof can be reversed to prove the "only if" part of the theorem.

ISOMORPHISM OF SYSTEMS

Construct the multiplication table for the non-zero elements of I/5 (arithmetic modulo 5). Designate this system by I/5*. (The * indicates that 0 has been omitted from I/5).

•	1	2	3	4
1				
2				
3		?		
4				

ANSWER:

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Construct the addition table for I/4.

+	0	1	2	3
0				
1		?		
2				
3				

ANSWER:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The above systems will be compared by setting up a function f which maps the elements of I/4 onto the elements of I/5*. To distinguish the elements of I/4 from those of I/5* we will underline the elements of I/5*. Thus the set of I/5* is $\{\underline{1}, \underline{2}, \underline{3}, \underline{4}\}$.

We begin defining the correspondence f by letting the identity element of I/4 correspond to the identity element of I/5*. In other words, ____ corresponds to ____.

ANSWER:

0 corresponds to $\underline{1}$.

We will designate the function in the following way:

$0 \xrightarrow{f} \underline{1}$

In I/4, if we add 2 + 2, the sum is 0. For which element of I/5* different from $\underline{1}$, is the *product* of the element with itself equal to the identity element $\underline{1}$?

ANSWER:

$\underline{4}$

Since 2 and $\underline{4}$ are similar in this respect we will let 2 correspond to $\underline{4}$. We will also let 1 correspond to $\underline{2}$ and 3 correspond to $\underline{3}$. Thus the function is defined as follows:

$$\begin{array}{llcl} & \underline{I/4} & & \underline{I/5^*} \\ f: & 0 & \longrightarrow & \underline{1} \\ & 1 & \longrightarrow & \underline{2} \\ & 2 & \longrightarrow & \underline{4} \\ & 3 & \longrightarrow & \underline{3} \end{array}$$

We have defined a function which has {0, 1, 2, 3} as its ____ and {$\underline{1}$, $\underline{2}$, $\underline{3}$, $\underline{4}$} as its ____.

- -

ANSWER:

domain

range

- -

We could have let 1 correspond to $\underline{3}$ and 3 correspond to $\underline{2}$. This would have given us the correspondence:

I/4		I/5*
0	⟶	$\underline{1}$
1	⟶	$\underline{3}$
2	⟶	$\underline{4}$
3	⟶	$\underline{2}$

A discussion similar to the one we will give for f could be given for this function also. You should observe that both of these functions are one-to-one (i.e., reversible) functions.

We return now to the function f (the first of the above two functions).

f(0) = _____

f(1) = _____

f(2) = _____

f(3) = _____

- -

ANSWER:

$\underline{1}$

$\underline{2}$

$\underline{4}$

$\underline{3}$

- -

Next consider the connection between this function and the binary operations.

$2 + 3 =$ ____

$f(2 + 3) =$ ____

$f(2) =$ ____

$f(3) =$ ____

$f(2) \cdot f(3) =$ ____

- -

ANSWER:

1

$f(2 + 3) = f(1) = \underline{2}$

$\underline{4}$

$\underline{3}$

$f(2) \cdot f(3) = \underline{4} \cdot \underline{3} = \underline{2}$

- -

Thus we see that $f(2 + 3) = f(2) \cdot f(3)$.

Which of the following statements are true?

a. $f(1 + 2) = f(1) \cdot f(2)$

b. $f(2 + 0) = f(2) \cdot f(0)$

c. $f(3 + 1) = f(3) \cdot f(1)$

d. $f(2 + 2) = f(2) \cdot f(2)$

- -

ANSWER:

All are true.

- -

We have tested five out of the sixteen possible ordered pairs (a, b) and have seen that $f(a + b) = f(a) \cdot f(b)$. It is possible to prove that this statement is true for all a and b by examining the remaining cases, but this will not be required.

We will instead reconstruct the table for multiplication in I/5* so that on the margins the elements of I/5* are in the same positions occupied by the corresponding elements of I/4 on that addition table. After the products are placed on the I/5* table we can compare it with the I/4 table.

I/4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

I/5*

$\cdot$	$\underline{1}$	$\underline{2}$	$\underline{4}$	$\underline{3}$
$\underline{1}$	$\underline{1}$	$\underline{2}$	$\underline{4}$	$\underline{3}$
$\underline{2}$	$\underline{2}$	$\underline{4}$	$\underline{3}$	$\underline{1}$
$\underline{4}$	$\underline{4}$	$\underline{3}$	$\underline{1}$	$\underline{2}$
$\underline{3}$	$\underline{3}$	$\underline{1}$	$\underline{2}$	$\underline{4}$

One can see by comparing the reconstructed table with the addition table for I/4 that the operation is preserved by the function f. For example, 2 corresponds to $\underline{4}$ and 2 occupies the positions on the I/4 table which correspond to the positions occupied by $\underline{4}$ on the I/5* table.

SUMMARY

We were able to determine a function from I/4 onto I/5* such that to each element of I/4 there is a unique element of I/5* to which it corresponds, and corresponding to each element of I/5* there is a unique element of I/4. Such a function is called a one-to-one correspondence between I/4 and I/5*. Furthermore, for all a, b in I/4, $f(a + b) = f(a) \cdot f(b)$.

DEFINITION 3.3: If G is a group whose operation is denoted by "o" and G' is a group whose operation is denoted by "Δ", then an isomorphism of the group G onto the group G' is a reversible function f from G onto G' such that:

$$f(a \circ b) = f(a) \, \Delta \, f(b)$$

for each a and b in G. We say that G and G' are isomorphic.

In the example discussed G is $I/4$ and the operation "o" is addition in $I/4$. The group G' is $I/5^*$ and the operation "Δ" is multiplication in $I/5^*$.

If two groups are isomorphic then they are algebraically equivalent. The elements which make up one group may be different from the elements which make up the other but any property possessed by the operation in one group will also be possessed by the other.

THEOREM 3.16: Let G be a group with operation "o" and G' a group with operation "Δ" and assume that f is an isomorphism of G onto G'. Then

1. If e is the identity element of G and $f(e) = e'$, then e' is the identity element of G'.
2. The image of the inverse of an element a of G is the inverse of the image of a. (i.e., if $f(a) = a'$, then $f(-a) = -(a')$, where $-a$ denotes the inverse of a in G and $-(a')$ denotes the inverse of a' in G'.)

PROOF:

Assume e is the identity element of G and $f(e) = e'$.
We must prove that ____.

ANSWER:

e' is the identity element of G'; or $e' \Delta a' = a' \Delta e' = a'$, for each a' in G'

Since e is the identity element of G we know that $e \circ a = a$ for each a in G. Let a' be an element of G' and let a be the element of G such that $f(a) = a'$.

By the definition of isomorphism we know that $f(a) = f(e \circ a) =$ ____.

ANSWER:

$f(e) \triangle f(a)$.

But $f(e) =$ ____ and $f(a) =$ ____.

ANSWER:

e'

a'

Therefore, $e' \triangle a' = a'$ for each a' in G'. Similarly, $a' \triangle e' = a'$ for each a' in G'. Thus e' is the ____ of G'.

ANSWER:

identity element

Let $f(-a) = (-a)'$. Note carefully the conceptual difference between $(-a)'$ and $-(a')$.

$(-a)' = f(-a)$ is the element of G' paired with the element $-a$ of G by the function f; $-(a') = -f(a)$ is the inverse in G' of the element paired with a by the function f. In order to prove that $f(-a) = -f(a)$ it is sufficient to show that

$f(a) \triangle f(-a) = e'$ and $f(-a) \triangle f(a) = e'$

Prove that $f(a) \triangle f(-a) = e'$.

ANSWER:

$f(a) \triangle f(-a) = f(a \circ [-a])$ because f is an isomorphism.

$a \circ [-a] = e$ since f is an isomorphism. Also, in the preceding proof it was shown that $f(e) = e'$, the identity element of G'. Therefore

$f(a) \;\Delta\; f(-a) = f(a \circ [-a]) = f(e) = e'$, i.e., $f(a) \;\Delta\; f(-a) = e'$.

Similarly, $f(-a) \;\Delta\; f(a) = e'$.

Theorem 3.16 is often useful in finding an isomorphism of one group onto another. The identity element of one group must correspond to the identity element of the other, and if two elements correspond their inverses must also correspond.

Find an isomorphism from the additive group of I/10 onto the multiplicative group of I/11*. (An element a of I/11* will be denoted $\underline{a}$.) Part of the mapping is already determined for you on the table given as an example given on the next page. Construct a function table and fill in the first column of blanks. (Ignore the blank table for I/11* and the second, third, and fourth columns of the function table.)

I/10

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

I/11*

·	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Function Table

I/10 I/11*

0 ⟶ ___ ___ ___ ___

1 ⟶ ___ ___ ___ ___

2 ⟶ ___ ___ ___ ___

3 ⟶ ___ ___ ___ ___

4 ⟶ ___ ___ ___ ___

5 ⟶ ___ ___ ___ ___

6 ⟶ ___ ___ ___ ___

7 ⟶ ___ ___ ___ ___

8 ⟶ ___ ___ ___ ___

9 ⟶ ___ ___ ___ ___

I/11*

·	
	?

- -

If you feel that you have given a complete solution go to †† on page 167. If you are not entirely satisfied with your solution go to the next item below.

- -

Using Theorem 3.16 you can arrive at the following assignments:

$0 \xrightarrow{f}$ ____

Since $1 \xrightarrow{f} 2$, ____ $\xrightarrow{f}$ ____.

ANSWER:

1

$9 \xrightarrow{f} 6$ since $-1 = 9$ and $2^{-1} = 6$. (We denote the inverse of 2 in I/11* by 2^{-1} instead of -2 since the operation in question is multiplication.)

If f is to be an isomorphism we must have $f(1 + 1) = f(1) \cdot f(1)$. In other words, $f(2) =$ ____.

ANSWER:

4

Go back to your solution. Make additions to, or changes in, the function table filling in the second column of blanks under I/11*. Do not write any more entries in the first column under I/11*.

If you feel that you have now given a complete solution go to †† on page 167. If not, go to the next item below.

We have set in correspondence the following pairs:

$0 \xrightarrow{f} 1$

$1 \xrightarrow{f} 2$

$2 \xrightarrow{f} 4$

$9 \xrightarrow{f} 6$

$f(1 + 2) = f(1) \cdot f(2) =$ ____.

Therefore $f(3) =$ ____.

- -

ANSWER:

8

8

- -

Continue this process until the correspondence is complete. Go back to your solution. Make additions to, or changes in, the function table using the third column under I/11*. Then go to the next item. Do not write any more entries in the first or second columns under I/11*.

- -

†† Does your solution agree with the following?

$0 \xrightarrow{f} \underline{1}$.

$1 \xrightarrow{f} \underline{2}$.

$6 \xrightarrow{f} \underline{9}$.

$9 \xrightarrow{f} \underline{6}$.

If you wish to do so, you may now go back to your solution and make any changes you like. List these in the fourth column of blanks. Do not make any changes or write any more entries in the first three columns. Then check you solution with the complete solution given below.

- -

Complete Solution:

	I/10		I/11*
f:	0	⟶	1
	1	⟶	2
	2	⟶	4
	3	⟶	8

$4 \longrightarrow \underline{5}$

$5 \longrightarrow \underline{10}$

$6 \longrightarrow \underline{9}$

$7 \longrightarrow \underline{7}$

$8 \longrightarrow \underline{3}$

$9 \longrightarrow \underline{6}$

The initial choice of the correspondence $1 \xrightarrow{f} \underline{2}$ is somewhat arbitrary in this example. We could construct an isomorphism by assigning 1 to any element of I/11* except for the element $\underline{1}$.

The function f is a reversible function from I/10 onto I/11*. To show that it is an isomorphism we must check that ____ for all a, b, in I/10.

ANSWER:

$f(a + b) = f(a) \cdot f(b)$

To provide this confirmation we will reconstruct the table for I/11* by placing the elements of I/11* in positions on the top and left sides of the table on page 165 which correspond to the positions occupied by the corresponding elements on the edges of the I/10 table. Thus the $\underline{4}$ on the I/11* table will be in a position corresponding to 2 on the I/10 table. After you have listed all of the elements on the edges of the I/11* table, complete the table by placing the respective products in the appropriate spaces. Use the given I/11* table for reference, if necessary.

I/11* (reconstructed)

·	1	2	4	8	5	10	9	7	3	6
1	1	2	4	8	5	10	9	7	3	6
2	2	4	8	5	10	9	7	3	6	1
4	4	8	5	10	9	7	3	6	1	2
8	8	5	10	9	7	3	6	1	2	4
5	5	10	9	7	3	6	1	2	4	8
10	10	9	7	3	6	1	2	4	8	5
9	9	7	3	6	1	2	4	8	5	10
7	7	3	6	1	2	4	8	5	10	9
3	3	6	1	2	4	8	5	10	9	7
6	6	1	2	4	8	5	10	9	7	3

- -

A comparison of the entries on the I/10 table with entries on the reconstructed I/11* table will confirm that this mapping is an isomorphism.

One other example of an isomorphism will be given in this section. Let P represent the group consisting of the positive real numbers and the multiplication operation. Let L be the group which is the set of all real numbers and the addition operation. Let f be the following function from P to L: $f(a) = \log_{10} a$ for each a in P. It can be shown that f is a reversible function from P onto L.

From your background in high school algebra you know

$f(a \cdot b) = \log_{10} (a \cdot b) =$ ____ + ____ = ____ + ____.

- -

ANSWER:

$\log_{10} a + \log_{10} b = f(a) + f(b)$

or $f(a) + f(b) = \log_{10} a + \log_{10} b$

- -

Therefore, as defined, f is an isomorphism from P onto L. Some interesting observations follow. For example: $f(1) =$ ____ since identities must correspond.

- -

ANSWER:

0

- -

Thus $f(1) = \log_{10} 1 = 0$.

Another interesting observation concerns division in R. (Recall $a \div b = a \cdot b^{-1}$).

Therefore,

$f(a \div b) = f(a \cdot b^{-1}) = f(a) + f(b^{-1})$.

But inverses are mapped onto inverses, thus

$f(b^{-1}) = -f(b) =$ ____.

- -

ANSWER:

$-\log_{10} b$. (This shows that $\log_{10} a \div b = \log_{10} a - \log_{10} b$.)

- -

A similar analysis would show that a^n corresponds to $n \cdot \log_{10} a$ for all integers n.

The definition of isomorphism can be extended to include mathematical systems with two or more operations. The following defintion would be suitable for an isomorphism from a field F onto a field F'.

DEFINITION 3.4: ϕ is an isomorphism of the field F with operations "+" and "·" onto the field F' with operations "$\oplus$" and "$\odot$" if:

1. ϕ is a one-to-one, or reversible function from F onto F',
2. $\phi(a + b) = \phi(a) \oplus \phi(b)$ for all a, b in F, and
3. $\phi(a \cdot b) = \phi(a) \odot \phi(b)$ for all a, b in F.

Further applications of the concept of isomorphism will be made later in the course.

REVIEW ITEMS

1. Consider the theorem:

Theorem: If a and b are real numbers, then $-(a - b) = b - a$.

Write the multiplicative analogue for the above theorem.

- -

ANSWER:

If a and b are non-zero real numbers then $(a/b)^{-1} = b/a$, or $(a \div b)^{-1} = b \div a$.

- -

2. Find the mistakes in the following proof.

Theorem: If A and B are non-zero 2×2 matrices, then $(A^{-1} \cdot B^{-1}) \cdot (A \cdot B) = I$.

PROOF:

1. A and B are non-zero 2×2 matrices — Hypothesis
2. A^{-1} and B^{-1} exist — M_{in}
3. $(A^{-1} \cdot B^{-1}) \cdot (A \cdot B) = (A^{-1} \cdot B^{-1}) \cdot (B \cdot A)$ — M_c
4. $= [(A^{-1} \cdot B^{-1}) \cdot B] \cdot A$ — M_a
5. $= [A^{-1} \cdot (B^{-1} \cdot B)] \cdot A$ — M_a
6. $= (A^{-1} \cdot I) \cdot A$ — M_{in}

7. $= A^{-1} \cdot A$ M_{id}

8. $= I$ M_{in}

- -

ANSWER:

Step (2) is not correct since M_{in} is not valid for 2×2 matrices. Step (3) is not valid since M_c is not valid for 2×2 matrices.

- -

3.

Prove or disprove: $a \div (b + c) = (a \div b) + (a \div c)$ for all real numbers a, b, and c where $b + c \neq 0$, $b \neq 0$ and $c \neq 0$.

- -

ANSWER:

This is a false theorem. One counter example is sufficient to disprove it.

Let $a = 6$ $\quad a \div (b + c) = 2$

$b = 2$ $\quad (a \div b) + (a \div c) = 9$

$c = 1$ $\quad \therefore \; a \div (b + c) \neq (a \div b) + (a \div c)$

Note that in fraction form this statement would be given as follows: $\frac{a}{b + c} = a/b + a/c$ which you recognize as a common error made by high school (and college) students.

- -

4. Let P, Q, R, and S denote the following matrices:

$$\begin{array}{cccc} P & Q & R & S \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \end{array}$$

Define the operation "*" in the following manner:

$X * Y = X \cdot R \cdot Y$ for all X and Y from the above set. In other words, to find $X * Y$ you find the matrix product of X, R, and Y where R is always the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

For example:

$$P * S = P \cdot R \cdot S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = Q.$$

(Recall that matrix multiplication is associative, thus the grouping one uses above is unimportant.)

Using the following example, construct an operation table for the set {P, Q, R, S} and the operation "*".

*	P	Q	R	S
P				
Q		?		
R				
S				

- -

ANSWER:

*	P	Q	R	S
P	R	S	P	Q
Q	S	R	Q	P
R	P	Q	R	S
S	Q	P	S	R

- -

Using the above table and any other information about matrix multiplication you find helpful, prove or disprove the following statement:

The set {P, Q, R, S} forms a group under the operation "*".

- -

ANSWER:

{P, Q, R, S} forms a group under the operation "*".

PROOF:

1. An examination of the table establishes closure for "*".

2. $*$ is an associative operation because matrix multiplication is associative. $(X * Y) * Z = (X \cdot R \cdot Y) * Z = (X \cdot R \cdot Y) R \cdot Z$ whereas $X * (Y * Z) = X * (Y \cdot R \cdot Z) = X \cdot R \cdot (Y \cdot R \cdot Z)$. These results are equal by the associative property of matrix multiplication.
3. R is the required identity element. (Refer to the table.)
4. $P^{-1} = P$
   $Q^{-1} = Q$
   $R^{-1} = R$
   $S^{-1} = S$

   (Refer to the table. $P * P = R$, $Q * Q = R$, etc.)

   Thus each element has an inverse.

Therefore {P, Q, R, S} forms a group under the operation "*".

- -

5. Given that {P, Q, R, S} forms a group under the operation "*", is this group isomorphic to the multiplicative group I/5*? Completely explain the reasons supporting your answer.

- -

ANSWER:

I/5*

•	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

*	P	Q	R	S
P	R	S	P	Q
Q	S	R	Q	P
R	P	Q	R	S
S	Q	P	S	R

These two groups are not isomorphic. One key is that each element in {P, Q, R, S} is a self-inverse whereas only 1 and 4 are self-inverses in I/5*. If you attempt to reconstruct the table for "*", you end up with the following contradiction:

	R	P
R	R	
P		R

Let R ↔ 1

and P, Q, or S ↔ 4

Wherever you place the other two elements, say Q and S, the elements on the diagonal of the table will equal R. But in the table for I/5* the diagonal elements are not always equal to 1. Thus the operation cannot be preserved under any one-to-one mapping.

IV. ORDER IN THE REAL NUMBER SYSTEM

ORDER POSTULATES

If you check the table of contents of a traditional high school mathemathics text you will likely find very few pages devoted to the topics of order and inequalities. In contrast, the S.M.S.G. Intermediate Mathematics Text Part I, 1960 Edition, has at least 38 pages of discussion and problems. Roy Dubisch in his Teacher's Guide to accompany his Introduction to Modern Algebra (D. Van Nostrand Company, Princeton, New Jersey, 1960, p. 100) says, "The student should certainly be informed that inequalities are used in mathematics almost as frequently as equalities".

In the development of the real number system as an example of a field we have so far encountered no properties which tell us the relative "size" of two numbers. You know that it makes sense to say that "12 is less than 16", that "-2 is less than 0", or that "1 is greater than 0"; but a review of the field properties and the theorems we have proved from them will show that you have not yet been given any logical basis for such statements about the relative order of two numbers.

In addition to the field postulates for the real numbers we will also assume that there is a "greater than" or "less than" relation having certain well defined properties. This assumption is stated formally as follows:

The field of real numbers is an ordered field in the sense that there is an order relation "<" in R which satisfies the four basic properties stated below. (The symbol "$a < b$" is read "a is less than b"; "$b > a$" is read "b is greater than a". We agree that $a < b$ and $b > a$ mean the same thing.)

ORDER PROPERTIES:

01 Trichotomy (or comparison) property:
If a and b are real numbers, then one and only of the following is true: $a < b$, $a = b$, $a > b$.

02 Transitive property:
If a, b, c are real numbers such that $a < b$ and $b < c$, then $a < c$.

03 Addition property:
If a, b, c are real numbers such that $a < b$, then $a + c < b + c$.

04 Multiplication property:
If a, b, c are real numbers such that $a < b$ and $0 < c$, then $ac < bc$.

The properties listed above are added to our list of postulates for the real number system.

In Unit I we defined a binary relation to be a set of ordered pairs. We can also regard the order relation introduced above as a set of ordered pairs. We define $\mathcal{O}$ to be the set of all ordered pairs (a, b) of real numbers a and b such that $a < b$ (or $b > a$). Then $\mathcal{O}$ is a binary relation according to the definition of Unit I.

The ordered pairs $(0, 1)$, $(2, 5)$, $(-2, -1)$, and $(-3, 2)$ are in the set $\mathcal{O}$ because we have $0 < 1$, $2 < 5$, $-2 < -1$, and $-3 < 2$. The ordered pairs $(0, -2)$, $(1, -3)$, and $(-8, -10)$ are not in $\mathcal{O}$ because it is not true that $0 < -2$ or $1 < -3$ or $-8 < -10$.

The basic properties 01, 02, 03, 04 can be restated for the set $\mathcal{O}$. Thus instead of writing "$a < b$" we write "(a, b) is in $\mathcal{O}$." The properties are restated as follows:

O1 Trichotomy (or comparison) property:

If a and b are real numbers, then one and only one of the following is true: (a, b) is in $\mathcal{O}$, $a = b$, (b, a) is in $\mathcal{O}$.

If you refer back to the previous statement of O1, you will note that the only change made is that "$a < b$" is replaced with "(a, b) is in $\mathcal{O}$", and "$a > b$" is replaced with "(b, a) is in $\mathcal{O}$".

Complete the following restatement of O2.

O2 Transitive property:

If a, b, c are real numbers such that (a, b) and (b, c) are in $\mathcal{O}$, then ____.

ANSWER:

(a, c) is in $\mathcal{O}$.

O3 Addition property

If a, b, c are real numbers such that ____, then ____.

ANSWER:

(a, b) is in $\mathcal{O}$.

$(a + c, b + c)$ is in $\mathcal{O}$.

O4 Multiplication property

Write out the Property O4.

ANSWER:

If a, b, c are real numbers such that (a, b) and $(0, c)$ are in $\mathcal{O}$, then (ac, bc) is in $\mathcal{O}$.

We will from time to time point out geometric interpretations of some of the order properties which we derive. It is often very helpful in solving inequalities to be able to translate a problem into geometric terms. We should say, however, that we make no attempt to establish a logical basis for the connection between the set of real numbers and the set of points on a line. To attempt to do so would take us beyond the scope of this course.

When we associate real numbers with points on a horizontal line in the usual way, if a and b are real numbers and $a < b$ then the point associated with a lies to the left of the point associated with b.

- -

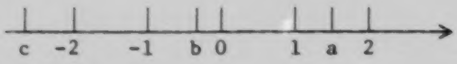


Figure 1

Refer to Figure 1 and tell which of the following statements is (are) true.

- -

(1) $b < 0$

- -

ANSWER:

True

- -

(2) $-2 > b$

- -

ANSWER:

False

- -

(3) (b, a) is in the set O.

- -

ANSWER:

True

- -

(4) (-2, a) is in the set O.

- -

ANSWER:

True

- -

If a, b, c are real numbers such that $a = b$, then $a + c = b + c$ because of the addition property of equality. Recall that this results from the fact that addition associates with each ordered pair of numbers a unique number. If $a = b$ then (a, c) and (b, c) are names for the same ordered pair; hence $a + c = b + c$. If a, b, c are real numbers such that $a < b$, then $a + c$ ___ $b + c$. Why?

- -

ANSWER:

<, by 03.

The addition property of equality is a theorem which follows from the definition of a binary operation, the assumption that addition is a binary operation, and the meaning of equality, but Property 03 must be regarded as a postulate.

- -

Note that the inequality "$a < b$" is not altered when a or b (or both) are replaced by equal quantities. As in the previous units we will make free use of this idea of "substitution" and will give no explicit reason when it is used, except where supplying the reason might prevent confusion.

Thus if $a = m$ and $b = x$, then the inequality $a < b$ may be replaced by the inequality ____ without comment.

- -

ANSWER:

$m < x$ (other answers: $a < x$, $m < b$)

- -

Reread the multiplication property, O4, for the "<" relation. Have any errors been made in applying it in the numerical examples below? Explain.

(1) Let $a = 4$, $b = 7$, $c = 2$, then $4 \cdot 2 < 7 \cdot 2$
(2) Let $a = 4$, $b = 7$, $c = 0$, then $4 \cdot 0 < 7 \cdot 0$
(3) Let $a = 4$, $b = 7$, $c = -2$, then $4(-2) < 7(-2)$
(4) Let $a = -7$, $b = -3$, $c = 2$, then $(-7)(2) < (-3)(2)$

- -

ANSWER:

(1) Correct: since $c > 0$, O4 applies.
(2) Wrong: since $c = 0$, O4 does not apply.
(3) Wrong: since $c < 0$, O4 does not apply.
(4) Correct: since $c > 0$, O4 applies.

- -

In terms of the order relation we shall make the following definitions for positive and negative numbers.

DEFINITION 4.1:

(1) A real number a is positive if and only if $a > 0$.
(2) A real number a is negative if and only if $a < 0$.

When 0 is substituted for b in the Trichotomy assumption, we have three alternatives for a real number a: $a < 0$, $a = 0$, and $a > 0$. This divides the real numbers into three non-overlapping subsets. What are they?

- -

ANSWER:

The set of negative real numbers,
$\{0\}$ (the set whose only member is zero), and
the set of positive real numbers.

- -

Note carefully that in Definition 4.1 no mention of a "minus sign" is made in the definition of negative number. Thus if we denote a number by $-a$ we are indicating the additive inverse of the number a. Use of the symbol $-a$ gives no indication as to whether the number in question is positive, negative, or zero. We shall see presently that if a is a positive number then $-a$ is a negative number, and that if a is a negative number then $-a$ is a positive number. We already know from Unit III that if a is zero then $-a$ is ____.

- -

ANSWER:

zero.

- -

We shall make frequent use of the set notation $\{x \mid \quad \}$ in which the defining conditions for x are written in the blank space. For example, $\{x \mid x > 4\}$ is read "the set of all x such that x is greater than 4".

We shall also refer to certain subsets of the real numbers in the following ways: Set of non-negative real numbers, set of positive real numbers, set of negative real numbers, set of non-positive real numbers.

Select the proper title for each of the following:

(1) $\{x \mid x > 0\}$

ANSWER:

(1) Set of positive real numbers.

---

(2) $\{x \mid x \not< 0\}$

ANSWER:

(2) Set of non-negative real numbers.

---

(3) $\{x \mid 0 < x\}$

ANSWER:

(3) Set of positive real numbers.

---

(4) $\{x \mid x < 0\}$

ANSWER:

(4) Set of negative real numbers.

---

(5) $\{x \mid x \geq 0\}$

ANSWER:

(5) Set of non-negative real numbers.

---

(6) $\{x \mid x \leq 0\}$

ANSWER:

(6) Set of non-positive real numbers.

Reminder: If a real number is not negative it is either _zero_ or a _positive_ number.

ORDER THEOREMS

There are many important theorems which follow as consequences of the order properties of real numbers. We shall state and prove a number of these theorems. In the beginning, in proving order theorems, you are asked to give complete proofs, showing each step in which you use either a field property or an order property of the real numbers. You may use the lists of field postulates and theorems given in the preceding units for reference. A little later you will be permitted to use the field properties without referring each time to the property which you are using. This will allow you to concentrate your attention on the order properties. Each time an order theorem is proved, it may then be used as a reason in a later proof.

THEOREM 4.1: If a, b, c, d are real numbers such that $a < b$ and $c < d$, then $a + c < b + d$.

The proof of this theorem is based on two order properties.

Suppose c is added to both members of the given inequality $a < b$. Write the inequality thus obtained.

Similarly, write the inequality obtained when b is added to both members of the given inequality, $c < d$.

These statements are justified by which order property?

ANSWER:

$a + c < b + c$

$c + b < d + b$

03 (addition)

What order property permits one to conclude from the two statements above that $a + c < b + d$?

ANSWER:

02 (transitive)

Using the preceding suggestions, write a complete proof for Theorem 4.1. Remember to list as reasons all field properties as well as order properties that you use.

ANSWER:

1. $a < b$, $c < d$, a, b, c, d are real numbers	Hypothesis
2. $a + c < b + c$	03
3. $c + b < d + b$	03
4. $b + c < b + d$	A_c
5. $a + c < b + d$	02

A theorem similar to Theorem 4.1 can be stated as a consequence of the multiplication property of order.

THEOREM 4.2: If a, b, c, and d are positive real numbers with $a < b$ and $c < d$, then $ac < bd$.

Give a numerical example to show that the above theorem is not true when the word positive is omitted.

ANSWER:

There are many examples; here are two:

(1) $-2 < -1$, and $-3 < 5$ but $(-2)(-3)$ is not less than $(-1)(5)$.

(2) $-4 < 0$, and $0 < 3$ but $(-4)(0)$ is not less than $(0)(3)$.

- -

The plan of proof for Theorem 4.2 is similar to that of Theorem 4.1. Write a complete proof for this theorem.

- -

ANSWER:

(1) $a < b$, $c < d$, a, b, c, d are positive real numbers	Hypothesis
(2) $c > 0$, $b > 0$	Definition 4.1
(3) $ac < bc$	04
(4) $cb < db$	04
(5) $bc < bd$	M_c
(6) $\therefore ac < bd$	02

You may count your proof as being correct even if you omitted step 2.

- -

From your past experiences in algebra you should be able to supply conclusions for the following statements. (Our next task will be to prove them.) For any real numbers a and b

(1) If $a < b$, then $a - b$ ___ 0. (Insert $<$ or $>$.)

(2) If $a > b$, then $a - b$ ___ 0.

(3) If $a - b > 0$, then a ___ b.

(4) If $a - b < 0$, then a ___ b.

- -

ANSWER:

(1) $<$, (2) $>$, (3) $>$, (4) $<$.

- -

The four statements from the preceding item are of the form, "If P then Q", where P and Q are statements. Thus the theorem "if $a < b$, then $a - b < 0$", has this form where P is the statement "$a < b$" and Q is the statement "$a - b < 0$". P is the hypothesis, or assumed part, of the statement and Q is the conclusion. The converse of a theorem is obtained by making the conclusion the hypothesis and by making the hypothesis the conclusion. (If the hypothesis or conclusion is a compound statement, a converse may be obtained by interchanging a "part" of each.) The converse of "If P then Q" is "If Q then P". The converse of "If $a < b$, then $a - b < 0$" is "If $a - b < 0$, then $a < b$".

Write the converses of the following theorems:

For any real numbers a and b,

(1) if $a > b$, then $a - b > 0$

(2) if $a + 3 = b$, then $b > a$.

- -

ANSWER:

For any real numbers a and b,

(1) if $a - b > 0$, then $a > b$.

(2) if $b > a$, then $a + 3 = b$.

- -

Consider the converses given in the previous item.

Does (1) appear to be true?

Does (2) appear to be true?

If a theorem is true, is its converse necessarily true?

- -

ANSWER:

The converse of Theorem (1) is true (the proof is given later). The converse of Theorem (2) is not true. There are numbers a and b such that $b > a$, but $a + 3 \neq b$; for example $a = 4$, $b = 10$.

If a theorem is true, its converse is not necessarily true.

THEOREM 4.3a: For any real numbers a and b, if $a < b$, then $a - b < 0$.

In proving this theorem recall that by definition of subtraction we can write $a - b$ in the form ___.

ANSWER:

$a + (-b)$

Give a complete proof of Theorem 4.3a using the addition assumption for inequalities; i.e., add $(-b)$ to both members of the inequality, $a < b$. Include a reason for the existence of $-b$.

ANSWER:

1.	$a < b$	Hypothesis
2.	$-b$ exists	A_{in}
3.	$a + (-b) < b + (-b)$	03
4.	$a - b < b + (-b)$	Definition of subtraction
5.	$a - b < 0$	A_{in}

Let us call the converse of Theorem 4.3a, Theorem 4.3b. State Theorem 4.3b and write a proof of it. Give a reason for each step in your proof. Remember to include field as well as order properties.

ANSWER:

THEOREM 4.3b: For any real numbers a and b if $a - b < 0$, then $a < b$.

PROOF:

1.	$a - b < 0$	Hypothesis

2.	$a + (-b) < 0$	Definition of subtraction
3.	$(a + (-b)) + b < 0 + b$	03
4.	$a + ((-b) + b) < 0 + b$	A_a
5.	$a + 0 < 0 + b$	A_{in}
6.	$a < b$	A_{id}

Since Theorem 4.3a and its converse are both true, they may be joined in a single statement as follows:

THEOREM 4.3: For real numbers a and b, $a < b$ *if and only if* $a - b < 0$.

The *if* part of this theorem is Theorem 4.3b and the *only if* part is Theorem 4.3a. State the corresponding theorem for $a > b$ in the if and only if form.

ANSWER:

THEOREM 4.4: For real numbers a and b, $a > b$ if and only if $a - b > 0$.

Using the proof of Theorem 4.3 as a guide, write a proof of Theorem 4.4. You should divide your answer into two parts - Theorem 4.4a, a statement and proof of the *only if* part of the theorem, and Theorem 4.4b, a statement and proof of the *if* part of the Theorem. Give reasons for all steps in your proof.

ANSWER:

THEOREM 4.4a: For any real numbers a and b, if $a > b$, then $a - b > 0$.

1.	$a > b$	Hypothesis

2.	$-b$ exists	A_{in}
3.	$a + (-b) > b + (-b)$	03
4.	$a - b > b + (-b)$	Definition of subtraction
5.	$a - b > 0$	A_{in}

THEOREM 4.4b: For any real numbers a and b, if $a - b > 0$, then $a > b$.

PROOF:

1.	$a - b > 0$	Hypothesis
2.	$a + (-b) > 0$	Definition of subtraction
3.	$(a + (-b)) + b > 0 + b$	03
4.	$a + ((-b) + b) > 0 + b$	A_a
5.	$a + 0 > 0 + b$	A_{in}
6.	$a > b$	A_{id}

It is worthwhile to note the geometric significance of the proofs of Theorems 4.3 and 4.4. For example, in Theorem 4.3a the hypothesis $a < b$ means that on the real line the point a is to the left of the point b. Adding a number c to both sides of the inequality $a < b$ translates each of the points a and b along the line in the same direction and the same distance. (We will return later in more detail to the consideration of distance on the line.) The translation is to the right if c is positive and to the left if c is negative. In the proof of Theorem 4.3a we choose $c = -b$. Then a is translated to $a - b$ and b is translated to $b - b = 0$. Therefore $a - b$ is to the left of 0; $a - b < 0$.

In proving the following theorems you may wish to make use of the List of Postulates and Theorems. Remember that you may use only the definitions, the basic order properties, the properties of a field, and the theorems preceding the one on which you are working.

THEOREM 4.5a: If b is a real number and $0 < b$, then $-b < 0$.

Write a proof of Theorem 4.5a using Theorem 4.3a. Give a reason for each step in your proof.

- -

ANSWER:

PROOF:

1.	$0 < b$	Hypothesis
2.	$0 - b < 0$	Theorem 4.3a
3.	$0 + (-b) < 0$	Definition of subtraction
4.	$-b < 0$	A_{id}

- -

State and prove the converse of Theorem 4.5a (which will be labeled Theorem 4.5b). Give a reason for each step in your proof.

- -

ANSWER:

THEOREM 4.5b: If b is a real number and $-b < 0$, then $b > 0$.

Here are three alternative proofs:

PROOF 1 (based on Theorem 4.4a):

1.	$0 > -b$	Hypothesis
2.	$0 - (-b) > 0$	Theorem 4.4a
3.	$0 + (-(-b)) > 0$	Definition of subtraction
4.	$0 + b > 0$	Field Theorem 3.5
5.	$b > 0$	A_{id}

PROOF 2 (based on Order Property 03):

1.	$-b < 0$	Hypothesis
2.	$(-b) + b < 0 + b$	03
3.	$0 < 0 + b$	A_{in}
4.	$0 < b$	A_{id}

PROOF 3 (based on Theorem 4.3b):

1.	$-b < 0$	Hypothesis
2.	$0 + (-b) < 0$	A_{id}
3.	$0 - b < 0$	Definition of subtraction

4. $0 < b$ Theorem 4.3b

- -

We have proved that Theorem 4.5a and its converse, Theorem 4.5b, are both true.

State a theorem which combines these two theorems. Label it Theorem 4.5.

- -

ANSWER:

THEOREM 4.5: For any real number b, $b > 0$ if and only if $-b < 0$.

- -

THEOREM 4.6a: If b is a real number, $b < 0$, then $-b > 0$.

Give a complete proof of this theorem.

- -

If you feel you have given a complete proof skip to the top of the next page. If not, go to the next item below.

- -

What field theorem is the justification for writing $b < 0$ in the form $-(-b) < 0$?

- -

ANSWER:

Theorem 3.5

Go back to your proof. Make additions or corrections before proceeding.

- -

(Complete proof of Theorem 4.6a is given on the following page.)

- -

ANSWER:

1.	$b < 0$	Hypothesis
2.	$-(-b) < 0$	Field Theorem 3.5
3.	$-b > 0$	Order Theorem 4.5

- -

P[illegible] the converse of Theorem 4.6a:

THEOREM 4.6b: If b is a real number and $-b > 0$, then $b < 0$.

- -

ANSWER:

PROOF:

1.	$-b > 0$	Hypothesis
2.	$-(-b) < 0$	Theorem 4.5
3.	$b < 0$	Field Theorem 3.5

- -

We combine Theorem 4.6a and 4.6b to obtain

THEOREM 4.6: For any real number b, $b < 0$ if and only if $-b > 0$.

As is clear from the proof, Theorem 4.6 is essentially the same as Theorem 4.5. It is only necessary to observe that $-(-b) = b$, which is Theorem 3.5.

Complete the examples below by stating the order relation of the given numbers and of their additive inverses:

(1) $3 < 5$ and $-3 > -5$

(2) -7 ____ -4 and ____

(3) 0 ____ 6 and ____

(4) If a and b are real numbers, $a < b$ if and only if $-b$ ____ $-a$.

- -

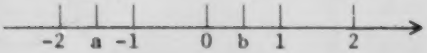
ANSWER:

(2) $-7 < -4$ and $-(-7) > -(-4)$, i.e., $7 > 4$.

(3) $0 < 6$ and $-0 > -6$, i.e., $-6 < 0$.

(4) $a < b$ if and only if $-b < -a$.

Suppose a and b are real numbers which are associated with points on a line as follows:



Mark each of the following statements as true or false.

(1) $-a$ is to the left of 0.

(2) $-a$ is to the right of $-b$.

(3) $-a$ lies between 0 and 1.

ANSWER:

(1) False

(2) True

(3) False

THEOREM 4.7: For real numbers a and b, $a < b$ if and only if $-b < -a$.

There are two statements to prove. What are they?

ANSWER:

(a) If a and b are real numbers and $a < b$, then $-b < -a$.

(b) If a and b are real numbers and $-b < -a$, then $a < b$.

To permit you to concentrate on the order properties of the real numbers you will no longer be asked to give as reasons in proofs the field properties that you use. You should continue however, to list order properties.

Write a proof for Theorem 4.7a.

ANSWER:

Two proofs are given below.

PROOF 1:

1.	$a < b$	Hypothesis
2.	$a - b < 0$	Theorem 4.3
3.	$-(a - b) > 0$	Theorem 4.6
4.	$-a - (-b) > 0$	
5.	$-a > -b$	Theorem 4.4

(Note that step 4 follows from step 3 by field properties. By our agreement to omit field properties as reasons, no reason is given for step 4.)

PROOF 2:

By hypothesis, $a < b$, so, by 03, $a + (-a) < b + (-a)$; i.e., $0 < b - a$. Again, by 03, $0 + (-b) < b - a + (-b)$; i.e., $-b < -a$. This is what was to be proved.

Write a proof of Theorem 4.7b, using Theorem 4.7a.

ANSWER:

PROOF:

1.	$-b < -a$	Hypothesis
2.	$-(-a) < -(-b)$	Theorem 4.7a
3.	$a < b$	

---

2 3

THEOREM 4.8: For real numbers a and b, if $a > 0$ and $b > 0$, then $a + b$ ____ 0.

THEOREM 4.9: For real numbers a and b, if $a < 0$ and $b < 0$, then $a + b$ ____ 0.

ANSWER:

> 0.

< 0.

Write a converse of Theorem 4.8.

Possible answers: For real numbers a and b,

(1) if $a + b > 0$, then $a > 0$ and $b > 0$.

(2) if $a + b > 0$ and $a > 0$, then $b > 0$.

(3) if $a + b > 0$ and $b > 0$, then $a > 0$.

Are any of these converses of Theorem 4.8 true?

ANSWER:

No.

Show how Theorems 4.8 and 4.9 follow directly from Theorem 4.1.

ANSWER:

Theorem 4.8: Since $a > 0$ and $b > 0$, by hypothesis, we can conclude from Theorem 4.1 that $a + b > 0 + 0$. Thus $a + b > 0$.

Theorem 4.9: By hypothesis, $0 > a$ and $0 > b$. By Theorem 4.1, $0 + 0 > a + b$; i.e., $0 > a + b$.

State a converse of Theorem 4.9. If you think your converse is true, prove it. If you think it is not true, give an example to disprove it.

Possible answer:

If $a + b < 0$, then $a < 0$ and $b < 0$.

Counter example: $(-9) + 2 < 0$ but $2 > 0$.

(There are other correct answers.)

Your familiarity with the "rules" for multiplication of positive and negative numbers should enable you to complete the theorems below.

THEOREM 4.10: If a and b are real numbers, $a > 0$ and $b > 0$, then $a \cdot b$ ____ 0.

THEOREM 4.11: If a and b are real numbers, $a < 0$ and $b < 0$, then $a \cdot b$ ____ 0.

THEOREM 4.12: If a and b are real numbers, $a > 0$ and $b < 0$, then $a \cdot b$ ____ 0.

ANSWER:

$>$

$>$

$<$

Criticize the following proof of Theorem 4.10.

PROOF: By hypothesis, $0 < a$ and $0 < b$. Hence, by Theorem 4.2,

$0 \cdot 0 < a \cdot b$; i.e., $0 < ab$.

ANSWER:

Theorem 4.2 is incorrectly applied. In the statement of Theorem 4.2, each of the numbers a, b, c, and d is assumed to be positive, hence not zero.

Give a correct proof of Theorem 4.10.

ANSWER:

PROOF:

1.	$a > 0,\ b > 0$	Hypothesis
2.	$ab > 0 \cdot b$	04, multiply by b
3.	$\therefore ab > 0$	

THEOREM 4.11: For real numbers a and b, if $a < 0$ and $b < 0$ then $ab > 0$. Can we apply the multiplication Property 04 immediately to prove Theorem 4.11? Explain.

ANSWER:

No. 04 applies only when we are multiplying by a positive number.

If $b < 0$ what do you know about $-b$? Give a reason.

ANSWER:

$-b > 0$, Theorem 4.6.

Write a proof for Theorem 4.11.

ANSWER: Two proofs:

PROOF 1:

1.	$a < 0, b < 0$	Hypothesis
2.	$-b > 0$	Theorem 4.6a
3.	$a(-b) < 0(-b)$	04
4.	$-(ab) < 0$	
5.	$\therefore ab > 0$	Theorem 4.5a

PROOF 2:

1.	$a < 0, b < 0$	Hypothesis
2.	$-a > 0, -b > 0$	Theorem 4.6
3.	$(-a)(-b) > 0$	Theorem 4.10
4.	Hence $ab > 0$	

Theorem 4.12 can be proved much as we have proved Theorems 4.10 and 4.11. We will not give a proof here.

We can use Theorems 4.10 and 4.11 to easily prove the following very important theorem.

THEOREM 4.13: If a is a real number and $a \neq 0$, then $a^2 > 0$.

If $a \neq 0$, we can conclude by Property 01 that ____.

ANSWER:

either $a > 0$ or $a < 0$.

Complete the proof of Theorem 4.13.

ANSWER:

If $a > 0$, then $a \cdot a > 0$ by Theorem 4.10. If $a < 0$, then $a \cdot a > 0$ by Theorem 4.11. Therefore, if $a \neq 0$, $a^2 = a \cdot a > 0$.

Since $1^2 = 1$, an immediate consequence of Theorem 4.13 is the fact that $1 > 0$. The statement "$1 > 0$" will perhaps not sound quite so trivial if stated in the following more general form:

In any ordered field the identity element for multiplication is greater than the identity element for addition.

Since $1 > 0$, it follows from Theorem 4.8 that $1 + 1 > 0$; i.e., $2 > 0$. Then similarly, $2 + 1 > 0$; i.e., $3 > 0$.

It can be shown by an extension of the above that all natural numbers are positive. Such a proof uses a principle called "mathematical induction". This principle will be introduced in a later unit and a proof that all natural numbers are positive will be given there.

Theorems 4.14, 4.15, 4.16 resemble the "cancellation" laws proved in Unit II. Relying again on your past experience, formulate a conclusion,

$a < b$, $a = b$, $a > b$, for each of the following:

THEOREM 4.14: For real numbers a, b, c, if $a + c < b + c$ then ____.

THEOREM 4.15: For real numbers a, b, c, if $ac < bc$ and $c > 0$ then ____.

THEOREM 4.16a: For real numbers a, b, c, if $ac < bc$ and $c < 0$ then ____.

ANSWER:

$a < b$.

$a < b$.

$a > b$.

In Theorem 4.14, is the conclusion true for all values of c (i.e., $c < 0$, $c = 0$, $c > 0$)?

ANSWER:

Yes.

Write a proof of Theorem 4.14. List as reasons all order properties that you use.

ANSWER:

PROOF:

1.	$a + c < b + c$	Hypothesis
2.	$-c$ exists	
3.	$(a + c) + (-c) < (b + c) + (-c)$	03
4.	$a < b$	

(In conformity with previous agreement the field properties used need not be listed. If you omitted only step 2, do not mark your proof incorrect.)

A converse of Theorem 4.14 is given by order Property ____.

ANSWER:

03

Theorem 4.15: If a, b, c are real numbers, $ac < bc$, and $c > 0$, then $a < b$.

Can you prove Theorem 4.15 directly using O4 in the way that Theorem 4.14 was proved using O3? Explain.

- -

ANSWER:

No. In using O4 directly to prove Theorem 4.15 you would like to multiply both sides of the inequality $ac < bc$ by c^{-1} to get $a < b$. However, we do not know that $c^{-1} > 0$ when $c > 0$. Although this is true it has not yet been proved.

- -

A direct proof of a theorem is one which starts with the hypothesis and proceeds step by step to the conclusion. The proof we have given for Theorem 4.14 is a good example of a direct proof. In giving an indirect proof of a theorem, one starts out by assuming that the conclusion of the theorem is false. Then one shows that this assumption leads to a false conclusion, or to some contradiction. This then proves that the conclusion of the theorem could not have been false. Of course the hypothesis of the theorem will be used at some step of the proof, but it will not generally be the first step. We will illustrate with a proof of Theorem 4.15.

Theorem 4.15 is a statement about real numbers a, b, c. The hypothesis of the theorem is ____.

- -

ANSWER:

$ac < bc$ and $c > 0$.

- -

The conclusion is ____.

- -

ANSWER:

$a < b$

- -

In an indirect proof of Theorem 4.15 the first step will be: assume that the conclusion is false, i.e., assume that $a < b$ is not true. Using O1 we can then conclude that ____.

- -

ANSWER:

either $a = b$ or $a > b$.

- -

The idea now is to show that either of the conditions $a = b$, $a > b$, will give a contradiction of the hypothesis. Complete the following proof of Theorem 4.15.

PROOF:

(1) Assume $a < b$ is not true.

(2) Then $a = b$ or $a > b$ by O1.

(3) If $a = b$, then $ac = bc$, but by O1 $ac = bc$ and $ac < bc$ are not both possible. So $a = b$ gives a contradiction of the hypothesis, $ac < bc$.

(4) If $a > b$ then

- -

ANSWER:

PROOF:

(1) Assume $a < b$ is not true.

(2) Then $a = b$ or $a > b$ by O1.

(3) If $a = b$ then $ac = bc$, but by O1 $ac = bc$ and $ac < bc$ are not both possible. So $a = b$ gives a contradiction of the hypothesis, $ac < bc$.

(4) If $a > b$ then $ac > bc$ by O4, since we have $c > 0$ by hypothesis. But by O1 $ac > bc$ and $ac < bc$ are not both pos-

sible. So $a > b$ gives a contradiction of the hypothesis $ac < bc$. (5) Since $a = b$ and $a > b$ both lead to contradictions we must have $a < b$.

A converse of Theorem 4.15 is given by order Property ____.

ANSWER:

04

The proof of Theorem 4.16a will be omitted.

If we multiply both sides of an inequality by a positive number the direction of inequality is preserved. This is the statement of Property 04. However, if we multiply both sides of an inequality by a negative number the direction of inequality is reversed. This is the statement of the following theorem, which is a converse of Theorem 4.16a.

Theorem 4.16b: For real numbers a, b, c, if $a > b$ and $c < 0$, then $ac < bc$.

Write a proof for this theorem.

ANSWER:

PROOF:

1.	$a > b, \quad c < 0$	Hypothesis
2.	$-c > 0$	Theorem 4.4
3.	$-ac > -bc$	04
4.	$ac < bc$	Theorem 4.7

We combine Theorems 4.16a and 4.16b to form

THEOREM 4.16: For real numbers a, b, c, with $c < 0$, $ac < bc$ if and only if $a > b$.

In planning a proof for Theorem 4.15 you saw the need for a theorem such as:
"If a number is positive then its multiplicative inverse is positive." This theorem and its "relative" are stated as follows:

THEOREM 4.17: If a is a real number and $a > 0$, then $1/a > 0$.

THEOREM 4.18: If a is a real number and $a < 0$, then $1/a < 0$.

To prove Theorem 4.17 we observe that $1/a \cdot a = 1$ and $0 \cdot a = 0$. Since $1 > 0$ we have $1/a \cdot a > 0 \cdot a$. Then by Theorem ____ we conclude that $1/a > 0$.

ANSWER:
4.15.

The proof of Theorem 4.18 will be omitted. Since the multiplicative inverse of $1/a$ is a, for any non-zero real number a, it follows immediately from Theorems 4.17 and 4.18 that if $1/a > 0$ then $a > 0$ and that if $1/a < 0$ then $a < 0$.

Notice that in the foregoing development we used Theorem 4.15 in the proof of Theorem 4.17. Theorem 4.15 was proved by showing that if $ac < bc$ and $c > 0$, then each of the assumptions $a = b$ and $a > b$ leads to a contradiction. Instead of this approach we could have first proved Theorem 4.17 by showing that if $a > 0$ then each of the assumptions $a^{-1} = 0$ and $a^{-1} < 0$ leads to a contradiction. Then we could have used Theorem 4.17 and 04 to prove Theorem 4.15.

THEOREM 4.19: For real numbers a and b, if $a > b > 0$ then $1/b > 1/a$.

The inequality $1/b > 1/a$ can be obtained by multiplying both sides of the inequality $a > b$ by ____.

- -

ANSWER:

$1/ab$, or $1/a \cdot 1/b$

- -

What theorems can be used to deduce that $1/a \cdot 1/b > 0$? Explain.

- -

ANSWER:

By hypohtesis $b > 0$ and $a > b$. Hence $a > 0$, by Property O2. Then, by Theorem 4.17, $1/a > 0$ and $1/b > 0$. Finally, by Theorem 4.10, $1/a \cdot 1/b > 0$.

- -

The following theorem provides a convenient technique for ordering two fractions.

THEOREM 4.20: If a, b, c, d are real numbers with $b > 0$ and $d > 0$, then $a/b > c/d$ if and only if $ad > bc$.

Prove the "only if" part of the theorem, i.e., if $b > 0$, $d > 0$, and $a/b > c/d$, then $ad > bc$.

- -

ANSWER:

PROOF:

1.	$a/b > c/d$, $b > 0$, $d > 0$	Hypothesis
2.	$bd > 0$	Theorem 4.10
3.	$a/b(bd) > c/d(bd)$	O4
4.	$ad > bc$	

- -

The proof of the "if" part of Theorem 4.20, i.e., if $b > 0$, $d > 0$, and $ad > bc$, then $a/b > c/d$, is essentially a reversal of the steps of the previous proof.

Write the proof.

ANSWER:

PROOF:

1.	$ad > bc,\quad b > 0,\quad d > 0$	Hypothesis
2.	$bd > 0$	Theorem 4.10
3.	$1/bd > 0$	Theorem 4.17
4.	$ad(1/bd) > bc(1/bd)$	O4
5.	$a/b > c/d$	

The following theorems may be added to your list for reference when you are solving problems in the next unit. Proofs of these theorems will not be given here.

THEOREM 4.21: For real numbers a and b if $ab > 0$, then $(a > 0$ and $b > 0)$ or $(a < 0$ and $b < 0)$.

THEOREM 4.22: For real numbers a and b if $ab < 0$, then $(a > 0$ and $b < 0)$ or $(a < 0$ and $b > 0)$.

THEOREM 4.23: For real numbers a and b, $ab > 0$ if and only if $a/b > 0$.

THEOREM 4.24: For real numbers a and b, $a/b > 0$ if and only if $(a > 0$ and $b > 0)$ or $(a < 0$ and $b < 0)$.

THEOREM 4.25: For real numbers a and b, $a/b < 0$ if and only if $(a < 0$ and $b > 0)$ or $(a > 0$ and $b < 0)$.

THEOREM 4.26: For real numbers a and b, if $a > b > 0$, then $a^2 > b^2$.

THEOREM 4.27: For real numbers a and b, if $a^2 > b^2$, $a > 0$, and $b > 0$, then $a > b$.

We have taken the real number system as our model of an ordered field. You will see in later sections that there are other examples of ordered fields. However, not all fields are ordered. Consider the system I/3 of integers modulo 3. Let us assume that this is an ordered field and show a contradiction.

By Theorem 4.13, $0 < 1$

Then by O3, $0 + 1 < 1 + 1$, i.e., $1 < 2$

Again by O3, $1 + 1 < 2 + 1$

We have reached a contradiction. Explain.

ANSWER:

In the system of integers modulo 3, $2 + 1 = 0$, $\therefore$ in step 3 we have $2 < 0$. But this contradicts the statement that if $0 < 1$ and $1 < 2$, then $0 < 2$ (the transitive property of order). Thus our assumption that the integers modulo 3 is an ordered field is not true.

Let a and b be real numbers, $b \neq 0$. Consider the following two statements:

(1) If a is negative and b is negative then a/b is positive.

(2) $-a/-b = a/b$

Do you think these two statements say essentially the same thing? Explain.

ANSWER:

The two statements are not the same. They are concerned with entirely different concepts. The notions of positive and negative depend upon order in the real number system. In statement (2) the minus signs have nothing to do with order. $-a$ and $-b$ are the additive inverses of a and b. The notion of additive inverse depends only upon the field properties, and therefore, it has meaning in systems which are not ordered. Statement (2) is true in any field. Statement (1) does not make sense unless the field is ordered.

The fact that not every field is ordered tells us that the notions of "positive" and "negative" for real numbers cannot be derived from the field properties alone but depend also upon the order assumptions. The statement "a negative number is a number which carries a minus sign" is not a definition of negative number. It is simply a statement about notation. The more fundamental use of the minus sign is to denote the additive inverse of a number and the notion of additive inverse depends only upon the field properties, not upon the order properties. To emphasize this point you might recall the situation in I/2, arithmetic modulo 2. In this arithmetic $-1 = 1$, but the minus sign denotes the additive inverse and has nothing to do with the notion of "negative number". Within the real number system, if a student is drilled in the idea that the minus sign always means "negative" then he will probably have a difficult time reconciling statements such as the following:

(1) The absolute value of any number is either positive or zero.

(2) If a is negative, the absolute value of a is $-a$.

Note that in the second statement $-a$ is a positive number, not a negative number.

REVIEW ITEMS

1. Insert the correct symbol ($<$, $>$), then prove the theorems. Use 04.

(a) If $0 < a < b$, then a^2 ____ b^2.

(b) If $b < a < 0$, then a^2 ____ b^2.

In your proofs you need not list field properties that you use but list order properties.

ANSWER:

(a) $a^2 < b^2$

PROOF:

(1) $0 < a, \quad a < b$	Hypothesis
(2) $0 < b$	02
(3) $a^2 < ab, \quad ab < b^2$	04
(4) $a^2 < b^2$	02

(b) $a^2 < b^2$; two proofs are shown.

PROOF 1:

(1) $b < a < 0$	Hypothesis
(2) $-b > -a > 0$	Theorem 4.7
(3) $a^2 < b^2$	Theorem (a) above.

PROOF 2:

(1) $b < a, \quad a < 0$	Hypothesis
(2) $b < 0$	02
(3) $-b > 0, \quad -a > 0$	Theorem 4.6
(4) $-b > -a$	Theorem 4.7
(5) $b^2 > ab, \quad ab > a^2$	04
(6) $b^2 > a^2$	02

---

2. A system with three elements 0, 1, a, having addition and multiplication tables as shown below is a field, i.e., all the field properties are satisfied.

+	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Is this system an ordered field? Prove your answer:

- -

ANSWER:

No.

PROOF: Assume that the field is ordered.

(1)	By Theorem 4.13	$0 < 1$
(2)	By O3	$0 + 1 < 1 + 1$
(3)	By A_{id} and definition of addition	$1 < a$
(4)	By O2	$0 < a$
(5)	By O3	$0 + 1 < a + 1$
(6)	By A_{id} and definition of addition	$1 < 0$

(7) From step (1) we have $0 < 1$ and from step (6) we have $1 < 0$. But by O1 these cannot both be true, hence we conclude that the system defined above is not ordered.

- -

3. Prove the following theorem. Justify each step by means of a field property or an order postulate. If a and b are real numbers, $a < 0$, $b < 0$, then $a + b < 0$.

- -

ANSWER:

PROOF:

(1)	$a < 0,\quad b < 0$	Hypothesis
(2)	$a + b < 0 + b$	O3
(3)	$a + b < b$	A_{id}
(4)	$a + b < 0$	O2

- -

4. Prove the following theorem, listing any order properties used in your proof. You may omit field properties.

If $ab > 0$, then ($a > 0$ and $b > 0$) or ($a < 0$ and $b < 0$). [Hint: Show first that $a = 0$ and $b = 0$ are both impossible if $ab > 0$. Then assume that one of the numbers, say a, satisfies $a < 0$. Show that $b > 0$ is impossible.]

- -

ANSWER:

PROOF:

(1) $ab > 0$, by hypothesis

(2) If either $a = 0$ or $b = 0$, then $ab = 0$ which by 01 is contrary to the hypothesis $ab > 0$. Hence neither a nor b is zero.

(3) If either a or b is positive, say $b > 0$, then by Theorem 4.12 if $a < 0$, $ab < 0$, which again by 01 contradicts the hypothesis $ab > 0$. Hence if either a or b is positive then the other is also positive.

(4) If either a or b is negative, say $b < 0$, then by Theorem 4.12 if $a > 0$, $ab < 0$, which by 01 contradicts the hypothesis $ab > 0$. Thus if either a or b is negative, the other is also negative. This also follows from steps (2) and (3). If neither a nor b is 0 or positive then, by 01, we must have $a < 0$ and $b < 0$.

(5) Since by 01 we must have either $a > 0$, $a = 0$, or $a < 0$, and must have either $b > 0$, $b = 0$, $b < 0$, we conclude that ($a > 0$ and $b > 0$) or ($a < 0$ and $b < 0$).

- -

5. Prove: If c is a positive real number such that $a + c = b$, then $a < b$. List all order properties used in your proof.

- -

ANSWER:

PROOF:

(1)	$0 < c$	Hypothesis
(2)	$0 + a < c + a$	03
(3)	$a < a + c$	
(4)	$a + c = b$	Hypothesis
(5)	$a < b$	

- -

6. Prove: If a is a real number and $a < 0$, then $1/a < 0$. Give order properties only as reasons. Use only theorems numbered 4.17 or lower.

- -

ANSWER: Two proofs are shown:

PROOF A:

(1) Since $a < 0$ by hypothesis, we know that $1/a$ exists.

(2) $(1/a)^2 > 0$ Theorem 4.13.

(3) $a(1/a)^2 < a \cdot 0$ Theorem 4.12

(4) $[a(1/a)]1/a < a \cdot 0$

(5) $1/a < 0$

PROOF B:

(1) $a < 0$ by hypothesis

(2) If $1/a = 0$ then $1/a \cdot a = 0 \cdot a = 0$.

But $1/a \cdot a = 1$, and $1 \neq 0$, hence this is impossible.

Thus the assumption $1/a = 0$ leads to a contradiction.

(3) If $1/a > 0$, then by Theorem 4.12 $a(1/a) < a \cdot 0$, i.e., $1 < 0$.

This is a contradiction by Theorem 4.13.

(4) Since $1/a = 0$ and $1/a > 0$ are impossible we conclude by 01 that $1/a < 0$.

SOLUTION OF EQUATIONS AND INEQUALITIES

One of the principal topics of algebra is the solution of equations. The Ball State Program describes the process of solving an equation as follows: "To solve an equation (or inequality) in x is to find all numbers which when substituted for x convert the equation to a true statement. The set of all such numbers is called the solution set." The S.M.S.G Program refers to equations and inequalities as open sentences and calls x a variable. The Illinois Program calls x a "pronumeral". In all of these programs the solution of an equation or inequality is defined as the set of all numbers each of which, if substituted for x, changes the equation to a true statement.

The approach to solving equations in the traditional curricula has tended to be a "rule book" approach. Our purpose in this unit is to provide a logical basis for solving equations and inequalities. We shall assume that we are seeking solutions in the field of real numbers, and therefore we will be able to use the field and order properties of the real numbers.

In solving an equation or inequality you may find it tedious to have to write out in detail every step with reasons; and if the aim were simply to find the solution set it would of course be absurd to require that the process of solution be given in such detail. The main purpose here, however, is to illustrate how the properties of the real number system are involved in the process of solution. In those problems where complete solutions are required you should be careful to do everything which is logically necessary in order to specify the solution set exactly. The example presented on the next page is broken down into steps so that you can see the logical detail.

Solve the equation $2x + 1 = x + 2$. Give a complete solution, including reasons.

Solution: Suppose that x is a real number, and that it is, in fact, a solution of the equation $2x + 1 = x + 2$.

(Note: As previously agreed we will use addition and multiplication facts for natural numbers without reasons; e.g., we can here replace 2 by $1 + 1$ since 2 is simply another notation for $1 + 1$.)

Fill in the blanks:

1. $2x + 1 = x + (1 + 1)$ Hypothesis
2. $2x + 1 = (x + 1) + 1$ ____
3. $2x = x + 1$ ____
4. $(1 + 1) \cdot x = x + 1$ ____
5. $1 \cdot x + 1 \cdot x = x + 1$ ____
6. $x + x = x + 1$ ____
7. $x = 1$ ____

- -

ANSWER:

2. A_a
3. Theorem 2.1
5. D
6. M_{id}
7. Theorem 2.1

- -

By using the field properties, we have shown that if x is a real number such that $2x + 1 = x + 2$ then $x = 1$. Notice, however, that our reasoning up to now is based on the assumption that x is some real number which is a solution of the equation. Therefore, before we can be certain that $\{1\}$ is the solution set we must prove that 1 is actually a solution of the equation. This can be done in two ways. We shall illustrate both. Fill in the blanks.

A. Suppose $x = 1$. Then

1. $x + x = x + 1$
2. $1 \cdot x + 1 \cdot x = x + 1$ M_{id}
3. $(1 + 1) \cdot x = x + 1$ ____
4. $2x = x + 1$
5. $2x + 1 = (x + 1) + 1$
6. $2x + 1 = x + (1 + 1)$ ____
7. $2x + 1 = x + 2$

Hence the solution set is $\{1\}$.

ANSWER:

3. D

6. A_a

Alternate Method:

B. Suppose $x = 1$. Then

1. $2x + 1 = 2 \cdot 1 + 1$
$= 2 + 1$ M_{id}
$= 1 + 2$ A_c
2. $x + 2 = 1 + 2$

Therefore

3. $2x + 1 = x + 2$

Hence the solution set is $\{1\}$.

Find the solution set for the equation $4x - 3 = 2x + 11$. Give the complete solution. Remember there are two parts to the solution: (1) you must find the "candidates" for the solution set, (2) you must prove that the candidates are solutions to the given equation. Present all the steps in your solution as clearly and precisely as possible. (Later items may direct you to make additions or corrections in your work, therefore you should place your answer close to the top of the space provided. Number the steps in your solution so that you can refer to them when making changes or additions.)

If you feel you have given a complete solution skip to $\boxed{\dagger\dagger}$ on page 219. If not, go to the next items below.

Here is a framework for part of the solution. Fill in the blank.

Suppose that x is a real number such that $4x - 3 = 2x + 11$.

1. $4x - 3 = 2x + 11$ Hypothesis
2. $4x + (-3) = 2x + 11$ ____

ANSWER:

Definition of subtraction.

Two possible procedures now would be: (a) Add 3 to both sides of the equation, or, (b) Change $2x + 11$ to a form which will permit you to use the cancellation property of addition to cancel -3 from both sides of the equation.

Go back to your solution. Make additions or corrections before proceeding.

If you have given a complete solution go to $\boxed{\dagger\dagger}$ on page 219. If not, go to the next items below.

Here is a continuation of the solution using two possible procedures. Fill in the blanks.

3. $[4x + (-3)] + 3 = (2x + 11) + 3$
4. $4x + [(-3) + 3] = 2x + (11 + 3)$ ____
5. $4x + 0 = 2x + (11 + 3)$ ____
6. $4x = 2x + (11 + 3)$ ____
7. $4x = 2x + 14$ ____

ANSWER:

4. A_a
5. A_{in}
6. A_{id}

Alternate procedure:

3. $4x + (-3) = (2x + 11) + 0$ ____
4. $4x + (-3) = (2x + 11) + (3 + [-3])$ ____
5. $4x + (-3) = [(2x + 11) + 3] + (-3)$ ____
6. $4x = (2x + 11) + 3$ ____
7. $4x = 2x + (11 + 3)$ ____
8. $4x = 2x + 14$

ANSWER:

3. A_{id}
4. A_{in}
5. A_a
6. Theorem 2.1
7. A_a

Try to change $4x$ into a form that will permit you to cancel $2x$ from each side of the equation $4x = 2x + 14$. Then use the cancellation property for multiplication.

Go back to your solution. Draw another line under your work and write the number 2 at the end of the line. Made additions or corrections in the space beneath. *Do not make changes in the work above the line*. Then go on to the next item.

- -

$\boxed{\dagger\dagger}$ Your solution may differ in some respects from the one given and still be correct. However, you should check carefully the following items:

(1) Did you use "definition of subtraction" as reason for writing "$4x - 3 = 4x + (-3)$"?

(2) Giving "combining like terms" as reason for "$2x + 2x = 4x$" is not correct. Property D is the key here.

(3) Were you careful to point out each place where you used the associative property?

(4) If all that you have done is to show that if x is a real number such that $4x - 3 = 2x + 11$, then $x = 7$, you have *not* completed the solution.

Go back to your solution. Draw a line across the page and write the number 3 at the end of the line. Make additions or corrections in the space beneath. *Do not make changes in the work above the line*. Then check your solution with the one given.

- -

Complete Solution:

Suppose that x is a real number such that $4x - 3 = 2x + 11$.

1.	$4x - 3 = 2x + 11$	Hypothesis
2.	$4x + (-3) = 2x + 11$	Definition of subtraction
3.	$[4x + (-3)] + 3 = (2x + 11) + 3$	Definition of subtraction
4.	$4x + [(-3) + 3] = 2x + (11 + 3)$	A_a

5. $4x + 0 = 2x + (11 + 3)$ A_{in}

6. $4x = 2x + (11 + 3)$ A_{id}

7. $4x = 2x + 14$

8. $(2 + 2)x = 2x + 14$

9. $2x + 2x = 2x + 14$ D

10. $2x = 14$ Theorem 2.1

11. $2x = 2 \cdot 7$

12. $x = 7$ Theorem 2.2

Steps 3 - 7 may be replaced by the following alternate proof:

3. $4x + (-3) = (2x + 11) + 0$ A_{id}

4. $4x + (-3) = (2x + 11) + [3 + (-3)]$ A_{in}

5. $4x + (-3) = [(2x + 11) + 3] + (-3)$ A_a

6. $4x = (2x + 11) + 3$ Theorem 2.1

7. $4x = 2x + (11 + 3)$ A_a

8. $4x = 2x + 14$

To complete the proof we need to show that if $x = 7$, then $4x - 3 = 2x + 11$. Two methods are shown:

Method 1:

1. $x = 7$ Hypothesis

2. $2x = 2 \cdot 7$

3. $2x = 14$

4. $2x + 2x = 2x + 14$

5. $(2 + 2)x = 2x + 14$ D

6. $4x = 2x + 14$

7. -3 exists A_{in}

8. $4x + (-3) = (2x + 14) + (-3)$

9. $4x - 3 = (2x + 14) + (-3)$ Definition of subtraction

10. $4x - 3 = [2x + (11 + 3)] + (-3)$

11. $4x - 3 = (2x + 11) + [3 + (-3)]$ A_a (applied twice)

12. $4x - 3 = (2x + 11) + 0$ A_{in}

13. $4x - 3 = 2x + 11$ A_{id}

Method 2:

1.	x	$= 7$	Hypothesis
2.	$4x - 3$	$= 4 \cdot 7 - 3$	
		$= 28 - 3$	
		$= 28 + (-3)$	Definition of subtraction
		$= (25 + 3) + (-3)$	
		$= 25 + [3 + (-3)]$	A_a
		$= 25 + 0$	A_{in}
		$= 25$	A_{id}
3.	$2x + 11$	$= 2 \cdot 7 + 11$	
		$= 14 + 11$	
		$= 25$	
4.	Therefore		
	$4x - 3$	$= 2x + 11$	

The solution set of the equation $4x - 3 = 2x + 11$ is the set $\{7\}$.

- -

The reasoning in the first part of the solution of an equation or inequality is directed toward identifying the possible "candidate" or "candidates" for membership in the solution set -- starting with the assumptions that the set contains at least one member, and that the members of the set are real numbers. The reasoning in the second part of the solution is directed toward proving that the candidates which have been identified do in fact satisfy the given equation (i.e., make it true.)

The second part of the solution may be carried out in many cases by reversing the steps in the proofs used in part one. It may also be carried out by replacing the variable in the original equation with each member of the tentative solution set and showing that each of the resulting "sentences" is true by carrying out the indicated operations. Taking the solution to the above equation for example:

If $x = 7$, then $4(7) - 3 =$ ____ and $2(7) + 11 =$ ____, so
____ = ____.

ANSWER:

25,

25,

$4x - 3 = 2x + 11$

In many algebra texts, carrying out the steps in the first part of the solution is called "solving" the equation, and the equation is considered "solved" when these steps are completed. The students is often required to "check" his work, but it is often not recognized that this is an essential part of the process of solution.

The process of "checking" the solution to the foregoing equation is sometimes carried out in the following way, by inserting the members of the solution set into the original equation.

$$\begin{aligned} 4 \cdot 7 - 3 &= 2 \cdot 7 + 11 \\ 28 - 3 &= 14 + 11 \\ 25 &= 25 \end{aligned}$$

Sometimes question marks are placed over all the equal signs except the last one to indicate that the equality is in question until the last step is reached. This method of setting down the "checking" process does not make clear what the chain of reasoning is. Upon first glance it appears that one is starting with the assumption that $4 \cdot 7 - 3 = 2 \cdot 7 + 11$ and proving that $25 = 25$. This would of course be nonsense. However, it would be acceptable to start with $25 = 25$ and prove by reversing the steps that $4 \cdot 7 - 3 = 2 \cdot 7 + 11$. Perhaps the clearest form for "checking" is the following:

$4 \cdot 7 - 3 = 28 - 3 = 25$

$2 \cdot 7 + 11 = 14 + 11 = 25$

Therefore,

$4 \cdot 7 - 3 = 2 \cdot 7 + 11$

The kind of reasoning used in solving equations is used in solving inequalities.

Find the solution set for the inequality $5x < 36 - x$. Give the complete solution, including reasons for each step.

- -

Have you given the second part of the solution? If not, you can do so by reversing the steps in the first part. If you do this be sure to give the correct reasons for the reversed steps.

Your solution should be concluded with a statement of the solution set.

Go back to your solution. Make any additions or corrections before proceeding.

- -

ANSWER:

Part 1. Suppose that x is a solution of the inequality $5x < 36 - x$.

1.	$5x < 36 - x$	Hypothesis
2.	$5x < 36 + (-x)$	Definition of Subtraction
3.	$5x + x < (36 + (-x)) + x$	O3
4.	$5x + x < 36 + ((-x) + x)$	A_a
5.	$5x + x < 36 + 0$	A_{in}
6.	$5x + x < 36$	A_{id}
7.	$5x + 1 \cdot x < 36$	M_{id}
8.	$(5 + 1)x < 36$	D
9.	$6x < 36$	
10.	$6x < 6 \cdot 6$	
11.	$x < 6$	Theorem 4.15

Part 2: If $x < 6$ then $5x < 36 - x$.

1.	$x < 6$	Hypothesis
2.	$6x < 6 \cdot 6$	04
3.	$(5 + 1)x < 36$	
4.	$5x + 1 \cdot x < 36$	D
5.	$5x + x < 36$	M_{id}
6.	$-x$ exists	A_{in}
7.	$(5x + x) + (-x) < 36 + (-x)$	03
8.	$5x + (x + (-x)) < 36 + (-x)$	A_{a}
9.	$5x + 0 < 36 + (-x)$	A_{in}
10.	$5x < 36 + (-x)$	A_{id}
11.	$5x < 36 - x$	Definition of subtraction

Hence the solution set is $\{x \mid x < 6\}$, i.e., the set of all x such that $x < 6$, (or the set of all real numbers less than six).

- -

It would be very tedious in the following to go on justifying each step in every proof. Therefore, in the remainder of this unit you may use the field properties without listing them, but continue to list the order properties.

Solve the inequality $-2x + 3 \geq -5$

- -

ANSWER:

Part 1. Suppose there is a real number x such that $-2x + 3 > -5$.

1.	$-2x + 3 > -5$	Hypothesis
2.	$(-2x + 3) + (-3) > -5 + (-3)$	03
3.	$-2x > -8$	
4.	$8 > 2x$	Theorem 4.7
5.	$4 > x$	Theorem 4.15

(An alternate method for steps 4 and 5 used Theorem 4.16 with $c = -2$.)

Part 2.

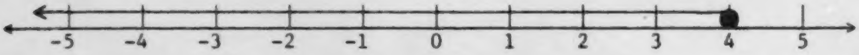
If $4 > x$ then $-2x + 3 > -5$.

1.	$4 > x$	Hypothesis
2.	$8 > 2x$	O4
3.	$-2x > -8$	Theorem 4.7
4.	$-2x + 3 > -8 + 5$	O3
5.	$-2x + 3 > -5$	

Hence the solution set is $\{x \mid 4 > x\}$.

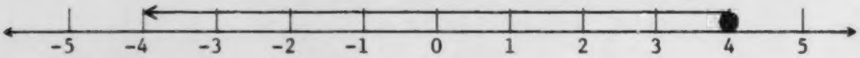
- -

The graph of the solution set for the inequality $-2x + 3 > -5$ is the set of all points on the number line whose coordinates are less than 4. This is the set of all points on the number line which lie to the left of the point whose coordinate is 4. The set is shown thus:



The sentence $-2x + 3 \geq -5$ is a compound sentence. It is interpreted as $-2x + 3 > -5$ or $-2x + 3 = -5$. The solution set must contain all the numbers which satisfy either of the conditions $x < 4$ or $x = 4$, hence the solution set is $\{x \mid 4 \geq x\}$.

The set is shown thus:



You can often carry out simultaneously both parts, (1) and (2), of a solution by showing that each step is reversible.

Consider, for example, the solution of the inequality $5x < -3x + 8$:

Step 1. by 03	$5x < -3x + 8$	Step 4. by 03
	$8x < 8$	
Step 2. by Theorem 4.15	$x < 1$	Step 3. by 04

$\therefore$ The solution set is $\{x \mid x < 1\}$.

The above can be written in the following compact form:

$5x < -3x + 8 \Longleftrightarrow 8x < 8$ By 03

$8x < 8 \Longleftrightarrow x < 1$ By Theorem 4.15 and 04

$\therefore$ The solution set is $\{x \mid x < 1\}$.

(The symbol $\Longleftrightarrow$ is read "if and only if".)

Write a solution for the inequality $(4y - 1) - 2(y + 1) > 0$ using the "if and only if" form. You may combine several steps when field properties only are involved. You need not list field properties used.

ANSWER:

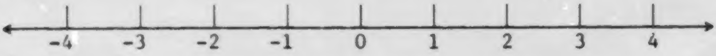
$(4y - 1) - 2(y + 1) > 0 \Longleftrightarrow 2y - 3 > 0$

$2y - 3 > 0 \Longleftrightarrow 2y > 3$ 03

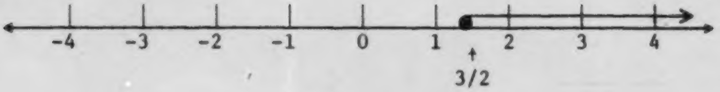
$2y > 3 \Longleftrightarrow y > 3/2$ Theorem 4.15

Hence the solution set is $\{y \mid y > 3/2\}$.

Show the solution set of the previous equation on the number line below.



ANSWER:



The sentence $2 < x + 3 < 6$ is equivalent to a compound sentence consisting of two inequalities ____ and ____.

ANSWER:

$2 < x + 3$

$x + 3 < 6$

Whenever two inequalities are combined in this way, $2 < x + 3 < 6$, it is always assumed that both inequalities hold.

To find the solution set we see that by order property O3

$2 < x + 3 \Leftrightarrow$ ____ and

$x + 3 < 6 \Leftrightarrow$ ____.

Hence the solution set is $\{x \mid$ ___ and ___$\}$.

ANSWER:

$-1 < x$

$x < 3$

$-1 < x$

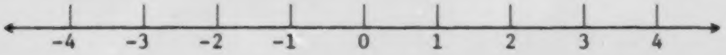
$x < 3$

The solution set for the previous problem is usually written thus, $\{x \mid -1 < x < 3\}$ and is read "the set of all x such that ____".

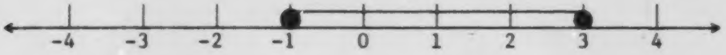
ANSWER:

x is greater than -1 and less than 3, or -1 is less than x and x is less than 3.

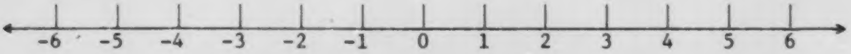
Indicate this set on the number line shown here:



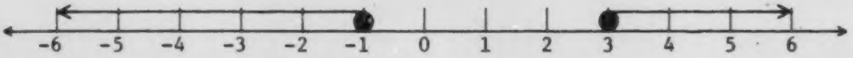
ANSWER:



We do not combine two inequalities into one statement of this kind when we wish to state that one or the other holds. For example, if we know that $x > 3$ or $x < -1$ we would not write $3 < x < -1$. The set of all x such that $x > 3$ or $x < -1$ in set notation is written $\{x \mid x > 3 \text{ or } x < -1\}$. Show this set on the number line below.


-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6

ANSWER:


-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6

Find the solution set for the inequality $7 < 5 - 2x \leq 15$.

You may omit the reasons in writing your solution, but show your work. Arrange your work in the "if and only if" form. (There are two inequalities to solve, $7 < 5 - 2x$ and $5 - 2x \leq 15$.)

- -

ANSWER:

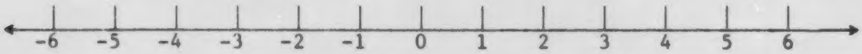
$7 < 5 - 2x \Leftrightarrow 2 < -2x$, and $5 - 2x \leq 15 \Leftrightarrow -2x \leq 10$.

$2 < -2x \Leftrightarrow x < -1$, and $-2x \leq 10 \Leftrightarrow x \geq -5$.

$\therefore$ The solution set is $\{x \mid -5 \leq x < -1\}$.

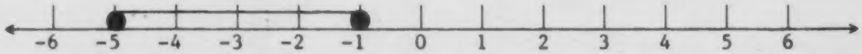
- -

Show the solution set of the preceding inequality on the number line below.



- -

ANSWER:



- -

Study the example below and fill in the blanks.

Find the values of x for which $x^2 - 5x + 6 > 0$.

$x^2 - 5x + 6 > 0 \Leftrightarrow (x - 2)(x - 3) > 0$

$(x - 2)(x - 3) > 0 \Leftrightarrow$ (1) $[(x - 2) > 0$ and $(x - 3) > 0]$ or (2) $[(x - 2) < 0$ and $(x - 3) < 0]$ by Theorem ____.

Case (1) $x - 2 > 0 \Leftrightarrow x > 2$, and $x - 3 > 0 \Leftrightarrow x > 3$.

Now $x > 2$ and $x > 3$ are both satisfied only when $x >$ ____.

Case (2) $x - 2 < 0 \Leftrightarrow x < 2$, and $x - 3 < 0 \Leftrightarrow x < 3$.

Here $x < 2$ and $x < 3$ are both satisifed only when ____.

$[(x - 2 > 0)$ and $(x - 3 > 0)]$ or $[(x - 2 < 0)$ and $(x - 3 < 0)]$

$\Leftrightarrow$ x ____ or x ____

Thus the solution set is {____}.

ANSWER:

Theorem 4.21

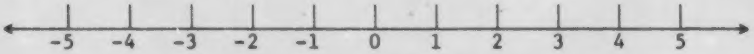
$x > 3$

$x < 2$

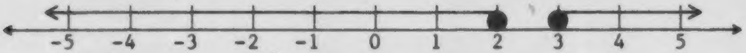
$x > 3$ or $x < 2$

$\{x \mid x > 3 \text{ or } x < 2\}$

Show the solution set $\{x \mid x > 3 \text{ or } x < 2\}$ on the number line below.



ANSWER:



The solution of the previous inequality may be arranged in the form of a chart as shown below. The first line of the chart has been completed to show that if x is less than 2, then the factor $x - 2$ is negative, the factor $x - 3$ is negative, and the product $(x -2)(x - 3)$ is positive.

Complete the second and third lines and the final statement.

	$x - 2$	$x - 3$	$(x - 2)(x - 3)$
If $x < 2$	Neg.	Neg.	Pos.
If $2 < x < 3$			
If $x > 3$			

$\therefore (x - 2)(x - 3) > 0 \Leftrightarrow$ ____.

- -

ANSWER:

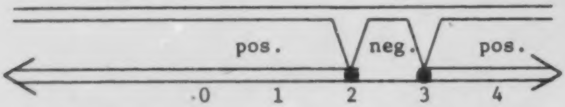
	$x - 2$	$x - 3$	$(x - 2)(x - 3)$
If $x < 2$	Neg.	Neg.	Pos.
If $2 < x < 3$	Pos.	Neg.	Neg.
If $x > 3$	Pos.	Pos.	**Pos.**

$x < 2$ or $x > 3$

Note that $(x - 2)(x - 3) = 0$ if $x = 2$ or if $x = 3$.

- -

The information from the chart can be shown graphically thus:



The chart also gives you the necessary information to state the solution set for the inequality $(x - 2)(x - 3) < 0$.

What is the solution set for $(x - 2)(x - 3) < 0$?

- -

ANSWER:

$\{x \mid 2 < x < 3\}$

- -

Consider the solution of $x^2 - 25 < 0$ outlined below:

$x^2 - 25 < 0 \iff (x - 5)(x + 5) < 0.$

By Theorem 4.22, $(x - 5)(x + 5) < 0 \iff$ (1) ____. or (2) ____.

- -

ANSWER:

(1) $x - 5 < 0$ and $x + 5 > 0$ or

(2) $x - 5 > 0$ and $x + 5 < 0$

- -

Therefore $(x - 5)(x + 5) < 0 \iff$ (1) $x < 5$ and $x > -5$ or (2) $x > 5$ and $x < -5$

Which one of the possibilities listed above must be rejected?

Give the solution set for the inequality $x^2 - 25 < 0$ in set notation.

- -

ANSWER:

The second possibility must be rejected since "$x > 5$ and $x < -5$" is not true for any value of x.

The solution set is $\{ x \mid -5 < x < 5\}$.

- -

Complete the solution below to find the solution of the inequality $12 < 2x^2 - 5x$.

$$12 < 2x^2 - 5x \iff 0 < 2x^2 - 5x - 12$$

$$2x^2 - 5x - 12 > 0 \iff (2x + 3)(x - 4) > 0$$

	$2x + 3$	$x - 4$	$(2x + 3)(x - 4)$
If $x < -3/2$			
If			
If			

The solution set is ____.

- -

ANSWER:

	$2x + 3$	$x - 4$	$(2x + 3)(x - 4)$
If $x < -3/2$	Neg.	Neg.	Pos.
If $-3/2 < x < 4$	Pos.	Neg.	Neg.
If $x > 4$	Pos.	Pos.	Pos.

$\{x \mid x < -3/2 \text{ or } x > 4\}$.

- -

If we change the "is less than" sign in the above problem to "is less than or is equal to" thus:

$12 \leq 2x^2 - 5x$, what is the solution set?

- -

ANSWER:

$\{x \mid x \leq -3/2 \text{ or } x \geq 4\}$.

- -

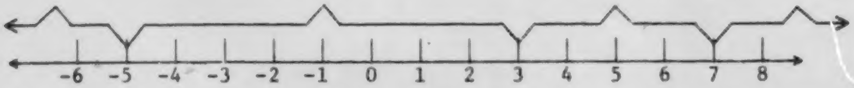
This example shows how to apply the foregoing techniques to more complicated problems.

Find the solution set of the inequality $(x + 5)(x - 3)(x - 7) \leq 0$ by completing the outline below.

1. $(x + 5)(x - 3)(x - 7) = 0 \Leftrightarrow x =$ ____, $x =$ ____, or $x =$ ____.

2.

	x + 5	x - 3	x - 7	(x + 5)(x - 3)(x - 7)
If $x < -5$				
If $-5 < x < 3$				
If $3 < x < 7$				
If $x > 7$				


-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6
7
8

Indicate the positive and negative sections on the graph above.

3. Hence $(x + 5)(x - 3)(x - 7) \leq 0 \Leftrightarrow$ ____.

The solution set is ____.

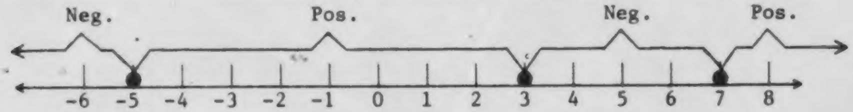
- -

ANSWER:

1. $-5, 3, 7$

2\.

	x + 5	x - 3	x - 7	(x + 5)(x - 3)(x - 7)
If $x < -5$	Neg.	Neg.	Neg.	Neg.
If $-5 < x < 3$	Pos.	Neg.	Neg.	Pos.
If $3 < x < 7$	Pos.	Pos.	Neg.	Neg.
If $x > 7$	Pos.	Pos.	Pos.	Pos.


Neg.
Pos.
Neg.
Pos.
-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6
7
8

3. $x \leq -5$ or $3 \leq x \leq 7$.

$\{x \mid x \leq -5$ or $3 \leq x \leq 7\}$, i.e., the set of all real numbers x such that either $x \leq -5$ or $3 \leq x \leq 7$.

- -

Find the solution set for $x + 1 > x + 2$. Show that the steps in your solution are reversible using the symbol $\Leftrightarrow$. You need not give reasons, but show the steps in your solution, using the "if and only if" form.

ANSWER:

$x + 1 > x + 2 \quad \Leftrightarrow \quad 0 > 1$

$\therefore$ The solution set has no members since $0 > 1$ is not true.

Find the solution set for $x + 1 = x + 1$. Show your work.

ANSWER:

$x + 1 = x + 1 \quad \Leftrightarrow \quad x - x = 1 - 1.$

$x - x = 1 - 1 \quad \Leftrightarrow \quad 0 = 0$

$\therefore$ The solution set is R, the set of all real numbers.

Solve the inequality $x^2 + 1 > 2x$. Show your work.

ANSWER:

$\{x \mid x \neq 1\}$ or $\{x \mid x > 1 \text{ or } x < 1\}$.

$x^2 + 1 > 2x \quad \Leftrightarrow \quad x^2 - 2x + 1 > 0.$

$x^2 - 2x + 1 > 0 \quad \Leftrightarrow \quad (x - 1)(x - 1) > 0.$

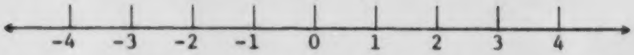
$\Leftrightarrow \quad [x - 1 > 0 \text{ and } x - 1 > 0]$ or

$[x - 1 < 0 \text{ and } x - 1 < 0].$

$\Leftrightarrow \quad x > 1$ or $x < 1$.

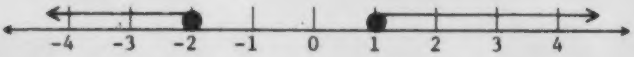
$\therefore$ The solution set is $\{x \mid x \neq 1\}$.

Indicate on the number line the set $\{x \mid x > 1 \text{ or } x < -2\}$.



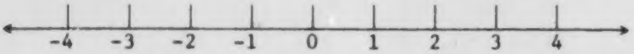
- -

ANSWER:



- -

Indicate on the number line the set $\{x \mid x > 1 \text{ and } x < -2\}$.



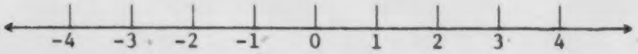
- -

ANSWER:

There are no numbers in the set since there is no number x such that $x > 1$ and $x < -2$.

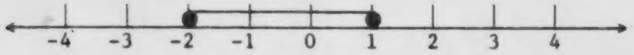
- -

Indicate on the number line the set $\{x \mid x < 1 \text{ and } x > -2\}$.



- -

ANSWER:



- -

An inequality requires a careful solution when the variable occurs in the denominator of a fraction. Consider the problem $\frac{x + 2}{3 - x} < 0$. In simplifying the inequality by "multiplying by the denominator" one has to worry about whether the denominator is positive or negative. This difficulty is avoided by the following solution.

By Theorem 4.25, $\frac{x+2}{3-x} < 0 \Leftrightarrow$ ____.

ANSWER:

(1) $[x + 2 < 0$ and $3 - x > 0]$ or

(2) $[x + 2 > 0$ and $3 - x < 0]$.

---

(1) $[x + 2 < 0$ and $3 - x > 0] \Leftrightarrow [x$ ____ and x ____$]$.

Thus to satisfy condition (1), x must be ____.

(2) $[x + 2 > 0$ and $3 - x < 0] \Leftrightarrow [x$ ____ and x ____$]$.

Thus to satisfy condition (2), x must be ____.

(3) Hence $\frac{x+2}{3-x} < 0 \Leftrightarrow$ ____.

(4) $\therefore$ The solution set is ____.

ANSWER:

(1) $x < -2$ and $x < 3$, x must be less than -2.

(2) $x > -2$ and $x > 3$, x must be greater than 3.

(3) $x < -2$ or $x > 3$.

(4) $\{x \mid x < -2$ or $x > 3\}$.

If x satisfies the conditions,

(1) $x > 0$ and $x > -2$, then ____.

(2) $x < 6$ and $x < 5$, then ____.

(3) $x > -2$ and $x < 3$, then ____.

(4) $x < 0$ and $x > 5$, then ____.

(5) $x \geq 1$ and $x \leq 1$, then ____.

ANSWER:

(1) $x > 0$.

(2) $x < 5$.

(3) $-2 < x < 3$.

(4) There are no values.

(5) $x = 1$.

- -

Solve the inequality $\frac{x - 2}{x + 5} > 0$. Show the steps in the solution and list the order theorem you use as a reason for your first step.

- -

ANSWER:

$$\frac{x - 2}{x + 5} > 0 \iff \left[\begin{array}{lll} & x - 2 > 0 \text{ and } & x + 5 > 0, \\ \text{or} & x - 2 < 0 \text{ and } & x + 5 < 0 \end{array}\right] \text{ by Theorem 4.24.}$$

$[x - 2 > 0 \text{ and } x + 5 > 0] \iff [x > 2 \text{ and } x > -5] \iff$
$x > 2$.

$[x - 2 < 0 \text{ and } x + 5 < 0] \iff [x < 2 \text{ and } x < -5] \iff$
$x < -5$.

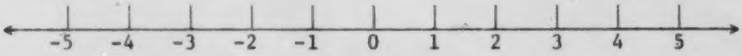
Hence $\frac{x - 2}{x + 5} > 0 \iff x > 2 \text{ or } x < -5$.

The solution set is $\{x \mid x > 2 \text{ or } x < -5\}$.

- -

What is the solution set for the inequality $\frac{3}{1 - x} < 0$?

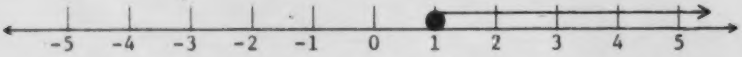
Indicate the solution set on the number line below.



- -

ANSWER:

$\{x \mid x > 1\}$.

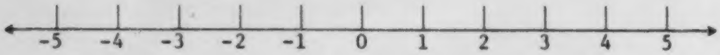


Note by Theorem 4.25, since 3 is greater than zero, there is only one case to consider; $\frac{3}{1 - x} < 0 \iff [3 > 0 \text{ and } 1 - x < 0]$
$\iff x > 1$.

- -

What is the solution set for the inequality $\frac{3}{1 - x} > 0$?

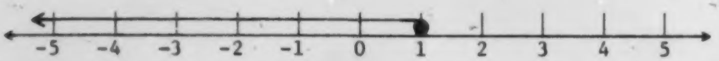
Indicate this set on the number line below.



- -

ANSWER:

$\{x \mid x < 1\}$.



- -

What are the real numbers in the solution set of the equation $\frac{3}{1 - x} = 0$?

- -

ANSWER:

There are no real numbers x such that $\frac{3}{1 - x} = 0$.

- -

Consider the inequality $\frac{2}{x - 1} > 3$. $(x - 1)$ may be negative or $(x - 1)$ may be positive, depending on the value of x, hence we must consider two possibilities. Two solutions will be given.

Solution 1:

$$\begin{aligned} \frac{2}{x - 1} > 3 &\Leftrightarrow \frac{2}{x - 1} - 3 > 0 \\ &\Leftrightarrow \frac{2 - 3x + 3}{x - 1} > 0 \\ &\Leftrightarrow \frac{5 - 3x}{x - 1} > 0. \end{aligned}$$

Complete the solution. What theorem is used in the next step?

- -

ANSWER:

By Theorem 4.24:

$$\frac{5-3x}{x-1} > 0 \Leftrightarrow \begin{cases} (1) & [5-3x>0 \text{ and } x-1>0] \Leftrightarrow \\ & [x<5/3 \text{ and } x>1] \Leftrightarrow [1<x<5/3], \text{ or} \\ (2) & [5-3x<0 \text{ and } x-1<0] \Leftrightarrow \\ & [x>5/3 \text{ and } x<1] \end{cases}$$

Since there is no real number x such that $x > 5/3$ and $x < 1$, the solution set is, from Case (1), $\{x \mid 1 < x < 5/3\}$

Solution 2: To solve the inequality $\frac{2}{x-1} > 3$ we consider the two cases $x - 1 > 0$ and $x - 1 < 0$ as follows:

Complete the solution of Case 1:

Case 1: $x - 1 > 0$ and $\frac{2}{x-1} > 3$ $\Leftrightarrow$ $x - 1 > 0$ and $2 > 3(x - 1)$ by Order Property ____.

Complete the solution of Case 2:

Case 2: $[x - 1 < 0$ and $\frac{2}{x-1} > 3]$ $\Leftrightarrow$ $[x - 1 < 0$ and $2 < 3(x - 1)]$ by Theorem ____.

Hence the solution set is ____.

ANSWER:

Case 1: Order Property 04.

$$\begin{aligned} [x-1>0 \text{ and } 2>3(x-1)] &\Leftrightarrow [x>1 \text{ and } 3x<5] \\ &\Leftrightarrow [x>1 \text{ and } x<5/3] \\ &\Leftrightarrow [1<x<5/3] \end{aligned}$$

Case 2: Theorem 4.16

$$\begin{aligned} [x-1<0 \text{ and } 2<3(x-1)] &\Leftrightarrow [x<1 \text{ and } 3x>5] \\ &\Leftrightarrow [x<1 \text{ and } x>5/3]. \end{aligned}$$

Since there is no real number x such that $x < 1$ and $x > 5/3$ the solution set, from Case 1, is the set $\{x \mid 1 < x < 5/3\}$.

- -

Find the values of x for which $\frac{3}{1 - x} < -2$ is true. (Solve the problem using either type of solution outlined in the preceding example. Show your work. No reasons are required.)

- -

ANSWER:

Solution 1:

$$\begin{aligned} \frac{3}{1 - x} < -2 \quad &\Leftrightarrow \quad \frac{3}{1 - x} + 2 < 0, \\ &\Leftrightarrow \quad \frac{3 + 2 - 2x}{1 - x} < 0, \\ &\Leftrightarrow \quad \frac{5 - 2x}{1 - x} < 0. \end{aligned}$$

There are two cases to consider: (1) $1 - x > 0$ and

(2) $1 - x < 0$.

$$\frac{5 - 2x}{1 - x} < 0 \quad \Leftrightarrow \quad \left\{ \begin{aligned} &(1)\ [5 - 2x < 0 \text{ and } 1 - x > 0], \\ \text{or } &(2)\ [5 - 2x > 0 \text{ and } 1 - x < 0]. \end{aligned} \right.$$

$$\Leftrightarrow \quad \left\{ \begin{aligned} &(1)\ [x > 5/2 \text{ and } x < 1], \\ \text{or } &(2)\ [x < 5/2 \text{ and } x > 1]. \end{aligned} \right.$$

Note: There is no real number x satisfying conditions (1) $[x > 5/2$ and $x < 1]$, but from (2) we obtain $1 < x < 5/2$.

$$\therefore \frac{3}{1 - x} < -2 \quad \Leftrightarrow \quad 1 < x < 5/2.$$

Hence the solution set is $\{x \mid 1 < x < 5/2\}$.

Solution 2: We consider two cases $1 - x > 0$ and $1 - x < 0$.

Case 1:

$$\begin{aligned} \left[1 - x > 0 \text{ and } \frac{3}{1 - x} < -2\right] \quad &\Leftrightarrow \quad [1 - x > 0 \text{ and } 3 < -2(1 - x)]. \\ &\Leftrightarrow \quad [1 > x \text{ and } 3 < -2 + 2x], \\ &\Leftrightarrow \quad [1 > x \text{ and } 5 < 2x], \\ &\Leftrightarrow \quad [1 > x \text{ and } 5/2 < x]. \end{aligned}$$

Case 1 is impossible since there is no real number x such that $x < 1$ and $x > 5/2$.

Case 2:

$$\begin{aligned}\left[1 - x < 0 \text{ and } \frac{3}{1 - x} < -2\right] &\leftrightarrow [1 < x \text{ and } 3 > -2(1 - x)],\\ &\leftrightarrow [1 < x \text{ and } 3 > -2 + 2x],\\ &\leftrightarrow [1 < x \text{ and } 5/2 > x],\\ &\leftrightarrow [1 < x < 5/2].\end{aligned}$$

Hence the solution set is $\{x \mid 1 < x < 5/2\}$.

Solve the inequality $\frac{x + 1}{x} > 2$. Show your work.

ANSWER:

Two solutions are shown.

Solution 1:

Case 1:

$$\begin{aligned}\left[x > 0 \text{ and } \frac{x + 1}{x} > 2\right] &\leftrightarrow [x > 0 \text{ and } x + 1 > 2x],\\ &\leftrightarrow [x > 0 \text{ and } 1 > x],\\ &\leftrightarrow [0 < x < 1].\end{aligned}$$

Case 2:

$$\begin{aligned}\left[x < 0 \text{ and } \frac{x + 1}{x} > 2\right] &\leftrightarrow [x < 0 \text{ and } x + 1 < 2x],\\ &\leftrightarrow [x < 0 \text{ and } 1 < x].\end{aligned}$$

Case 2 is impossible.

Hence the solution set is $\{x \mid 0 < x < 1\}$.

Solution 2:

$$\begin{aligned}\frac{x + 1}{x} > 2 \leftrightarrow \frac{x + 1}{x} - 2 > 0 &\leftrightarrow \frac{x + 1 - 2x}{x} > 0\\ &\leftrightarrow \frac{1 - x}{x} > 0\end{aligned}$$

$$\Leftrightarrow \left\{ \begin{array}{ll} & [(1 - x) > 0 \quad \text{and} \quad x > 0] \\ \text{or} & [(1 - x) < 0 \quad \text{and} \quad x < 0] \end{array} \right\}$$

$$\Leftrightarrow \left\{ \begin{bmatrix} 1 > x \quad \text{and} \quad x > 0 \\ \text{i.e.,} \quad 0 < x < 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 < x \quad \text{and} \quad x < 0 \\ \text{(impossible)} \end{bmatrix} \right\}$$

Hence the solution set is $\{x \mid 0 < x < 1\}$.

- -

Solve the inequality $1 > x^2$. Show your work.

- -

ANSWER:

(1) $\{x \mid -1 < x < 1\}$

Solution:

$$\begin{array}{ll} 1 > x^2 & \Leftrightarrow \quad 0 > x^2 - 1 \\ & \Leftrightarrow \quad 0 > (x - 1)(x + 1) \\ & \Leftrightarrow \left\{ \begin{array}{ll} & [(x - 1) < 0 \quad \text{and} \quad (x + 1) > 0] \\ \text{or} & [x - 1 > 0 \quad \text{and} \quad (x + 1) < 0] \end{array} \right. \\ & \Leftrightarrow \left\{ \begin{array}{ll} & [x < 1 \quad \text{and} \quad x > -1] \\ \text{or} & [x > 1 \quad \text{and} \quad x < -1] \text{ (impossible)} \end{array} \right. \\ & \Leftrightarrow \quad -1 < x < 1 \end{array}$$

	$x + 1$	$x - 1$	$(x - 1)(x + 1)$
$x < -1$	Neg.	Neg.	Pos.
$-1 < x < 1$	Pos.	Neg.	Neg.
$x > 1$	Pos.	Pos.	Pos.

Hence $1 > x^2 \Leftrightarrow -1 < x < 1$

The solution set is $\{x \mid -1 < x < 1\}$.

- -

Is the following true?

$1/x^2 > 1 \Leftrightarrow 1 > x^2$

- -

ANSWER:

No. Reread 04. This assumption holds only when $c > 0$. $x = 0$ is an element of the solution set of $1 > x^2$, but $1/x^2 > 1$ has no meaning when $x = 0$.

Solve the inequality $1/x^2 > 1$. Show your work.

ANSWER:

Since $x^2 \geq 0$ for all real numbers x, we do not "worry" about changing the direction of the inequality if $x < 0$, however $1/x^2$ is undefined at $x = 0$, therefore $1/x^2 > 1 \iff [x \neq 0$ and $1 > x^2]$. Now refer to the previous problem for the rest of the solution. $\{x \mid -1 < x < 0 \text{ or } 0 < x < 1\}$ (The solution set consists of all real numbers between -1 and 1, except 0.)

At each step in the process of solving an equation (or inequality) we replace one statement by another. As you have seen in the previous problem the replacement may not yield a statement which is the "same", in terms of the solution set, as the given one. This leads to the concept of equivalent equations or inequalities.

DEFINITION 5.1: Two equations or inequalities are said to be equivalent if and only if they have the same solution set.

When a rule of algebra is applied to transform an equation or inequality the resulting equation or inequality may or may not be equivalent to the original one. Some transformations, however, always result in an equivalent statement.

In solving an equation or inequality, a step in which the given statement is transformed into an equivalent one is said to be reversible.

(1) Is $4 = 28 - 12x$ equivalent to $-1 = -7 + 3x$?

Is this step reversible?

(2) Is $2x + 1 < 3$ equivalent to $2x < 2$?

Is this step reversible?

ANSWER:

(1) Yes

Yes

(2) Yes

Yes

Addition of a non-zero constant to both sides of an equation or inequality yields an equivalent result. Similarly, multiplication of an equation by a non-zero constant or multiplication of an inequality by a positive constant gives an equivalent equation or inequality.

Now consider the example where $\frac{1}{1 - x}$ has been added to both members of an equation.

Is $2x + 1 = 3$ equivalent to $2x + 1 + \frac{1}{1 - x} = 3 + \frac{1}{1 - x}$?

ANSWER:

No, the solution set of the first equation is $\{1\}$ while the second equation has no member in the solution set. [$\frac{1}{1 - x}$ is not defined when $x = 1$. Addition of $\frac{1}{1 - x}$ to both sides of the equation is not a reversible step.]

When an expression involving the variable x is added or multiplied on both sides of an equation or inequality the resulting statement may not be equivalent to the original.

Is $2x + 1 = 3$ equivalent to $(x - 1)(2x + 1) = 3(x - 1)$?

ANSWER:

Yes, the solution set for each equation is $\{1\}$. (Reread the definition for equivalent equations.) Note in this example, multiplication by an expression involving the variable did not "change" the solution set.

Is $2x + 1 = 3$ equivalent to $x(2x + 1) = 3x$?

ANSWER:

No, $x = 0$ satisfies the second equation but not the first.

Is $2x + 1 = 3$ equivalent to $4(2x + 1) = 12$?

ANSWER:

Yes, the solution sets are the same. Multiplying each side of the equation by 4 results in an equivalent equation.

Is $5x/8 \geq x + 3$ equivalent to $5x \geq 8x + 24$?

ANSWER:

Yes, both have the solution set $\{x \mid x \leq -8\}$.

The student should be aware that one of four different results may be produced when an equation or inequality is transformed by use of the multiplication properties. Let S be the solution set for the original and S' be the solution set for the transformed equation or inequality. Then

(1) $S = S'$ or

(2) $S \subset S'$, $S \neq S'$, or

(3) $S' \subset S$, $S' \neq S$, or

(4) $S \not\subset S'$, and $S' \not\subset S$.

Consider the equation obtained from $\frac{x + 3}{x - 1} = \frac{8}{x - 1}$ when both members are multiplied by $(x - 1)^2$. The solution set for the derived equation $(x - 1)(x + 3) = 8(x - 1)$ is $S' =$ ____. The solution set for the original equation is $S =$ ____. Are the equations equivalent?

ANSWER:

$\{5, 1\}$; $\{5\}$.

No, this is a case where $S \subset S'$, $S \neq S'$.

Consider the equation obtained from $x - 5 + 4/x = 0$ when both members of the equation are multiplied by x.

(1) The solution set $S' =$ ____.

(2) The solution set $S =$ ____.

(3) In this example S ____ S'.

ANSWER:

(1) $\{4, 1\}$.

(2) $\{4, 1\}$.

(3) $=$ the equations are equivalent.

Consider the inequality obtained from $1/x > -1$ when both members are multiplied by x.

The solution set for $1/x > -1$ is $S =$ ____.

The solution set for $1 > -x$ is $S' =$ ____.

In this example S ____ S'.

ANSWER:

$S = \{x \mid x < -1 \text{ or } x > 0\}$.

$S' = \{x \mid x > -1\}$.

$S \not\subset S'$, and $S' \not\subset S$.

Consider the equation obtained from $\sqrt{x + 3} = 1 + x$ when you square both of its members.

(1) The solution set $S' =$ ____.

(2) The solution set $S =$ ____.

(3) Are these equations equivalent?

ANSWER:

(1) $\{-2, 1\}$.

(2) $\{1\}$.

(3) No.

The following are some "morals" to be drawn from this discussion.

If all the steps in the solution of an equation or inequality are reversible you may use the symbol $\Longleftrightarrow$ in writing the solution and no further check is necessary.

If certain steps are not reversible then you must check the possible exceptions.

You must be sure that you have not performed operations in your solution that are invalid.

Complete the solution for the following problem: Find the values of x for which $-1 < \frac{x - 1}{x + 1} < 3$ is true. You may omit reasons, but show your work. The answer should be in set notation.

Step 1.

$$-1 < \frac{x-1}{x+1} < 3 \quad \Longleftrightarrow \quad -1 < \frac{x-1}{x+1} \ \underline{\text{and}} \ \frac{x-1}{x+1} < 3$$

There are two cases:

Case 1: $x + 1 > 0$. or

Case 2: $x + 1 < 0$.

- -

ANSWER:

Two solutions will be shown.

Solution 1:

$$\left[-1 < \frac{x-1}{x+1} \ \text{and} \ \frac{x-1}{x+1} < 3\right] \ — \ \left[0 < \frac{2x}{x+1} \ \text{and} \ \frac{-2x-4}{x+1} < 0\right]$$

Case 1: $x + 1 > 0$

$\Longleftrightarrow$ $[(x + 1 > 0 \ \text{and} \ 2x > 0) \ \text{and} \ (x + 1 > 0 \ \text{and} \ -2x - 4 < 0)]$

$\Longleftrightarrow$ $[(x > -1 \ \text{and} \ x > 0) \ \text{and} \ (x > -1 \ \text{and} \ -2 < x)]$

$\Longleftrightarrow$ $[x > 0 \ \text{and} \ x > -1]$

$\Longleftrightarrow$ $[x > 0]$

or

Case 2: $x + 1 < 0$.

$\Longleftrightarrow$ $[(x + 1 < 0 \ \text{and} \ 2x < 0) \ \text{and} \ (x + 1 < 0 \ \text{and} \ -2x - 4 > 0)]$

$\Longleftrightarrow$ $[(x < -1 \ \text{and} \ x < 0) \ \text{and} \ (x < -1 \ \text{and} \ -2 > x)]$

$\Longleftrightarrow$ $[x < -1 \ \text{and} \ x < -2]$

$\Longleftrightarrow$ $[x < -2]$

Hence the solution set is $\{x \mid x < -2 \ \text{or} \ x > 0\}$.

Solution 2: $-1 < \dfrac{x-1}{x+1}$ and $\dfrac{x-1}{x+1} < 3$

Case 1:

$\Longleftrightarrow$ $\left[\left(x + 1 > 0 \ \text{and} \ -1 < \dfrac{x-1}{x+1}\right) \ \text{and} \ \left(x + 1 > 0 \ \text{and} \ \dfrac{x-1}{x+1} < 3\right)\right]$

$\Longleftrightarrow$ $[(x + 1 > 0 \ \text{and} \ -x - 1 < x - 1) \ \text{and} \ (x + 1 > 0 \ \text{and} \ x - 1 < 3x + 3)]$

$\Longleftrightarrow$ $[x > -1 \ \text{and} \ 0 < x \ \text{and} \ -2 < x]$

$\Longleftrightarrow$ $[x > 0]$

or

Case 2:

$\Leftrightarrow$ $\left[\left(x + 1 < 0 \text{ and } -1 < \frac{x - 1}{x + 1}\right) \text{ and } \left(x + 1 < 0 \text{ and } \frac{x - 1}{x + 1} < 3\right)\right]$

$\Leftrightarrow$ $[(x + 1 < 0 \text{ and } -x - 1 > x - 1) \text{ and } (x + 1 < 0 \text{ and } x - 1 > 3x + 3)]$

$\Leftrightarrow$ $[x < -1 \text{ and } 0 > x \text{ and } -2 > x]$

$\Leftrightarrow$ $[x < -2]$

Hence the solution set is $\{x \mid x < -2 \text{ or } x > 0\}$.

We now wish to illustrate some of the complications that can arise in solving equations over a system which does not possess all of the field properties. This will emphasize how important these properties are in some of the routine work which we do with equations. We will consider the system of all 2×2 matrices of real numbers. Recall that the multiplication of two such matrices is carried out in the following manner:

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} = \begin{bmatrix} \quad & \quad \\ \quad & \quad \end{bmatrix}$$

ANSWER:

$$\begin{bmatrix} (2 \cdot 3) + (1 \cdot 1) & (2 \cdot 5) + (1 \cdot 6) \\ (3 \cdot 3) + (4 \cdot 1) & (3 \cdot 5) + (4 \cdot 6) \end{bmatrix} = \begin{bmatrix} 7 & 16 \\ 13 & 39 \end{bmatrix}$$

What multiplicative field properties are not possessed by matrix multiplication?

ANSWER:

M_c, M_{in}.

Recall that the real number equation $a \cdot x = b$ could be solved using basic field properties by multiplying both sides of the equation by ____.

- -

ANSWER:

a^{-1}. (This is possible, of course, only if $a \neq 0$.)

- -

A unique solution to the above equation exists for all real numbers a and b except $a = 0$. However, several complications arise when we try to solve the equation $A \cdot X = B$ where A and B are matrices and $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

For example, does the following equation have a solution X, where X is a 2×2 matrix? Explain how you arrived at your answer.

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} X = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

- -

ANSWER:

No. By the way matrix multiplication is defined, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} X$ could not have a non-zero element in its second row, regardless of what the matrix X is.

- -

Therefore, we see that not every equation of the form $AX = B$, with $A \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, has a solution. Show that if A has a multiplicative inverse then $AX = B$ has the unique solution $A^{-1}B$.

Part 1. Show that if $A \cdot X = B$, $X = A^{-1} \cdot B$.

Part 2. Show that if $X = A^{-1} \cdot B$, $A \cdot X = B$.

- -

ANSWER:

Part 1. Since $A \cdot X = B$, we have $A^{-1} \cdot (A \cdot X) = A^{-1} \cdot B$. $A^{-1} \cdot (A \cdot X) = (A^{-1} \cdot A) \cdot X = I \cdot X = X$ (where I is the identity matrix).

$\therefore X = A^{-1} \cdot B$.

Part 2. Let $X = A^{-1} \cdot B$.

Then $A \cdot (A^{-1} \cdot B) = (A \cdot A^{-1}) \cdot B = I \cdot B = B$.

Thus $A^{-1} \cdot B$ is the unique solution of the equation $A \cdot X = B$, where A has a multiplicative inverse.

- -

The absence of the field property ____ prevents one from proving that $B \cdot A^{-1}$ is also, in general, a solution of the equation $A \cdot X = B$.

- -

ANSWER:

M_c.

- -

Suppose A has a multiplicative inverse. Would B/A be a good notation for the solution $A^{-1} \cdot B$ of the equation $A \cdot X = B$? Why or why not?

- -

ANSWER:

No, since multiplication is not commutative in general, $A^{-1} \cdot B$ and $B \cdot A^{-1}$ are not necessarily equal. B/A could represent $A^{-1} \cdot B$ or $B \cdot A^{-1}$ and this would have a double meaning in some cases.

- -

For real numbers the equation $ax = b$ is equivalent to $xa = b$ because of the commutative law for multiplication. However M_c does not hold for matrices. If A has a multiplicative inverse, what is the unique solution of $XA = B$?

- -

ANSWER:

$X = BA^{-1}$.

- -

Recall from Unit III that if $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $ad - bc \neq 0$, then

$A^{-1} = \begin{bmatrix} & \\ & \end{bmatrix}$

- -

ANSWER:

$$A^{-1} = \begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$$

- -

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. What is A^{-1} ?

- -

ANSWER:

$A^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

- -

Let $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Using the results obtained in the above item find the solutions of the equations $AX = B$ and $XA = B$.

- -

ANSWER:

$AX = B : X = A^{-1}B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

$XA = B : X = BA^{-1} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

- -

This example shows that $AX = B$ and $XA = B$ may not be equivalent.

A more complicated linear equation is one which has the form $A_1XA_2 = B$. If both A_1 and A_2 have inverses, then the unique solution of this equation is $X =$ ____.

- -

ANSWER:

$X = A_1^{-1}BA_2^{-1}$

Note that $A_1^{-1}A_2^{-1}B$, $BA_1^{-1}A_2^{-1}$, etc., are not correct answers since matrix multiplication is not commutative in general. For example, if we take $X = A_1^{-1}A_2^{-1}B$, then

$A_1XA_2 = A_1A_1^{-1}A_2^{-1}BA_2 = IA_2^{-1}BA_2 = A_2^{-1}BA_2.$

Since BA_2 and A_2B may not be the same we cannot conclude that $A_1XA_2 = B$.

- -

The situation is even more complicated for quadratic equations. Over the field of real numbers every quadratic equation is equivalent to an equation of the form $ax^2 + bx + c = 0$, with $a \neq 0$.

Quadratic equations over the system of 2×2 matrices may have very complicated forms compared with quadratic equations over the field of real numbers. For example, we may have equations of the form $A_1XA_2XA_3 + B_1XB_2 + C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, where A_1, A_2, and A_3 are different from the zero matrix, and this is not the most general form. If, in the given equation, we let each of the matrices A_2, A_3, and B_2 equal the identity matrix, I, the equation reduces to the form ____.

- -

ANSWER:

$A_1X^2 + B_1X + C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Recall $A_1X \cdot I \cdot X \cdot I = A_1X^2$, etc.

- -

The proof of the quadratic formula depends upon the field properties M_c and M_{in} so that it does not hold in general for matrix equations even if the equation has the form $A_1X^2 + B_1X + C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Even the simple quadratic equation $X^2 = A$ leads to difficulties. There may be no solutions or many solutions.

The following example will illustrate one of these possibilities. Let $X = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ and $A = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$. Then if $X^2 = A$, we can write the following matrix equation:

$$\begin{bmatrix} \quad & \quad \\ \quad & \quad \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$$

- -

ANSWER:

$$\begin{bmatrix} x^2 + yz & xy + yw \\ zx + wz & zy + w^2 \end{bmatrix}$$

- -

Since two matrices are equal only if their corresponding elements are equal we can arrive at the following system of four real number equations:

- -

ANSWER:

(1) $x^2 + yz = -1$

(2) $xy + yw = 1$

(3) $zx + wz = 1$

(4) $zy + w^2 = 0$

- -

From equations (2) and (3), $y = \_\_\_\_$ and $z = \_\_\_\_$.

- -

ANSWER:

$$\frac{1}{x + w}$$

$$\frac{1}{x + w}$$

- -

Therefore $y = z$. In what way does this requirement introduce an inconsistency in the above system of equations? [Hint: Look at equation (1).]

- -

ANSWER:

If $y = z$, equation (1) can be written $x^2 + y^2 = -1$. But $x^2 + y^2 \geq 0$ and $-1 < 0$, thus the sytem of equations is inconsistent.

- -

Therefore we must conclude that the equation $X^2 = \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$ has no solution.

On the other hand, if a is any real number and $X = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$, we know $X^2 =$

- -

ANSWER:

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

- -

Therefore the equation $X^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ has many solutions as evidenced by the above choices for X.

Solution of polynomial matrix equations by factoring also involves certain difficulties. If in solving a real number quadratic equation we can arrive at the statement $(x - a)(x - b) = 0$, we can further conclude that ____ or ____.

ANSWER:

$x - a = 0$, $x - b = 0$

(or $x = a$, $x = b$).

This procedure is dependent on the property given in Theorem 2.4. In the proof of Theorem 2.4 we used the property M_{in}. This should cause us to be suspicious of this procedure if we attempt to apply it to matrix equations. The following example will support our suspicions. Let $A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Show by substitution and evaluation that the identity matrix, I, is a solution of the equation $(X - A) \cdot (X - B) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

ANSWER:

$$\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

But $I - A = \begin{bmatrix} & \end{bmatrix}$ and $I - B = \begin{bmatrix} & \end{bmatrix}$

ANSWER:

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

Thus $(I - A)(I - B) = 0$, but $(I - A) \neq 0$ and $(I - B) \neq 0$.

As we have observed in the preceding material the solution of a matrix equation cannot, in general, be arrived at through use of the techniques we use regularly in solving real number equations. This is due primarily to the failure of M_c and M_{in} to hold for the matrix operations. For the same reason, many familiar factoring formulas fail to hold over the system of 2×2 matrices. To illustrate this point we will consider the following example:

Expand the expression $(X - A)^2$. (Recall that matrix operations have all of the field properties except M_c and M_{in}.)

$(X - A)^2 =$

ANSWER:

$$(X - A)^2 = (X - A) \cdot (X - A) = X(X - A) - A(X - A)$$
$$= X^2 - XA - AX + A^2.$$

In order to illustrate that this is not equal to $X^2 - 2AX + A^2$ we will consider the following results: (Note: We define $2AX$ to mean $AX + AX$.)

Let $X = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ and $A = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$.

Compute $X^2 - X \cdot A - A \cdot X + A^2$.

ANSWER:

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \cdot$$
$$\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Compute $X^2 - 2AX + A^2$ for the given X and A.

ANSWER:

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} -2\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} - 2\begin{vmatrix} 0 & 0 \\ 1 & 1 \end{vmatrix} + \begin{vmatrix} 0 & 0 \\ 1 & 1 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} - \begin{vmatrix} 0 & 0 \\ 2 & 2 \end{vmatrix} + \begin{vmatrix} 0 & 0 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ -1 & -1 \end{vmatrix}$$

- -

The two results are not equal. Thus in general $(X - A)^2 \neq X^2 - 2AX + A^2$.

REVIEW ITEMS

Find solution sets in the following problems. Show your work.

1. $x^2 - 1/4 \leq 0$

- -

ANSWER:
$\{x \mid -1/2 \leq x \leq 1/2\}$
Solution:

$$x^2 - 1/4 \leq 0 \Leftrightarrow (x - 1/2)(x + 1/2) \leq 0$$

$$\Leftrightarrow \begin{array}{l} (x - 1/2) \leq 0 \text{ and } (x + 1/2) \geq 0 \text{ or} \\ (x - 1/2) \geq 0 \text{ and } (x + 1/2) \leq 0 \end{array}$$

$$\Leftrightarrow \begin{array}{l} x \leq 1/2 \text{ and } x \geq -1/2 \text{ or} \\ x \geq 1/2 \text{ and } x \leq -1/2 \text{ (impossible)} \end{array}$$

Hence the solution set is $\{x \mid -1/2 \leq x \leq 1/2\}$.

- -

2. $x^2 + 25 < 0$

- -

ANSWER:
No real values for x.
Solution: $x^2 + 25 < 0 \Leftrightarrow x^2 < -25$

Since $x^2 \geq 0$ for all real numbers, there are no real numbers such that $x^2 + 25 < 0$.

- -

3. $5x - x^2 > 0$

ANSWER:

$\{x \mid 0 < x < 5\}$

Solution:

$$5x - x^2 > 0 \iff x(5 - x) > 0$$

$$\iff \begin{cases} x > 0 \text{ and } 5 - x > 0 \text{ or} \\ x < 0 \text{ and } 5 - x < 0 \end{cases}$$

$$\iff \begin{cases} x > 0 \text{ and } 5 > x \text{ or} \\ x < 0 \text{ and } 5 < x \text{ (impossible)} \end{cases}$$

Hence the solution set is $\{x \mid 0 < x < 5\}$.

---

4. $\dfrac{x - 2}{x} > 0$

ANSWER:

$\{x \mid x < 0 \text{ or } x > 2\}$

Solution:

$$\frac{x - 2}{x} > 0 \iff \begin{cases} x > 0 \text{ and } x - 2 > 0 \text{ or} \\ x < 0 \text{ and } x - 2 < 0 \end{cases}$$

$$\iff \begin{cases} x > 0 \text{ and } x > 2 \text{ or} \\ x < 0 \text{ and } x < 2 \end{cases}$$

$$\iff \begin{cases} x > 2 \text{ or} \\ x < 0 \end{cases}$$

Hence the solution set is $\{x \mid x < 0 \text{ or } x > 2\}$.

---

5. $-1 < 3x + 2 < 17$

ANSWER:

$\{x \mid -1 < x < 5\}$

Solution:

$$-1 < 3x + 2 < 17 \iff -3 < 3x < 15$$
$$\iff -1 < x < 5$$

Hence the solution set is $\{x \mid -1 < x < 5\}$.

- -

6. $(x + 1)(x - 3)(2x - 3) > 0$

- -

ANSWER:

$\{x \mid -1 < x < 3/2 \text{ or } x > 3\}$.

Solution:

	$x + 1$	$2x - 3$	$x - 3$	$(x + 1)(2x - 3)(x - 3)$
$x < -1$	Neg.	Neg.	Neg.	Neg.
$-1 < x < 3/2$	Pos.	Neg.	Neg.	Pos.
$3/2 < x < 3$	Pos.	Pos.	Neg.	Neg.
$x > 3$	Pos.	Pos.	Pos.	Pos.

The table shows that $(x + 1)(2x - 3)(x - 3)$ is positive if and only if $-1 < x < 3/2$ or $x > 3$, hence the solution set is $\{x \mid -1 < x < 3/2 \text{ or } x > 3\}$.

- -

7. Let $A = \begin{bmatrix} 2 & 5 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Show whether or not the equations $AX = B$ and $XA = B$ are equivalent.

- -

ANSWER:

Part 1.

$A^{-1} = \begin{bmatrix} 0 & 1 \\ 1/5 & -2/5 \end{bmatrix}$

$$\begin{bmatrix} 2 & 5 \\ 1 & 0 \end{bmatrix} X = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Leftrightarrow \begin{bmatrix} 0 & 1 \\ 1/5 & -2/5 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 0 \end{bmatrix} X = \begin{bmatrix} 0 & 1 \\ 1/5 & -2/5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot X = \begin{bmatrix} 0 & 1 \\ 1/5 & -1/5 \end{bmatrix}$$

$$\Leftrightarrow X = \begin{bmatrix} 0 & 1 \\ 1/5 & -1/5 \end{bmatrix}$$

Part 2.

$$X \cdot \begin{bmatrix} 2 & 5 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Leftrightarrow X \begin{bmatrix} 2 & 5 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1/5 & -2/5 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1/5 & -2/5 \end{bmatrix}$$

$$\Leftrightarrow X \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1/5 & 3/5 \\ 1/5 & -2/5 \end{bmatrix}$$

$$\Leftrightarrow X = \begin{bmatrix} 1/5 & 3/5 \\ 1/5 & -2/5 \end{bmatrix}$$

The equations are not equivalent since they do not have the same solution sets. The solution set for $AX = B$ is $\left\{ \begin{bmatrix} 0 & 1 \\ 1/5 & -1/5 \end{bmatrix} \right\}$. The solution set for $XA = B$ is $\left\{ \begin{bmatrix} 1/5 & 3/5 \\ 1/5 & -2/5 \end{bmatrix} \right\}$.

- -

VI. ABSOLUTE VALUE

ABSOLUTE VALUE

Many students beginning a course in calculus have difficulty understanding definitions and explanations which involve the use of absolute values. Material in this unit should prove very helpful to the student who expects to take mathematics courses beyond the high school level. It is especially useful in connection with the study of limits in calculus.

DEFINITION 6.1: The absolute value $|a|$ of a real number a is defined thus:

$|a| = a$, if $a > 0$;
$|a| = 0$, if $a = 0$;
$|a| = -a$, if $a < 0$.

(1) Refer to the third part of the definition. Is the absolute value of a, when $a < 0$, a negative or a positive real number?

(2) Supply the correct numerical values:

If $x = 4$, then $|x| =$ ____
If $x = 0$, then $|x| =$ ____
If $x = -4$, then $|x| =$ ____

ANSWER:

(1) Positive, (see example below).

(2) 4
0
4

Note: $-(-4) = 4$

- -

Give numerical answers for the following:

(a) $|5 - 2| =$ ____ (b) $|2 - 5| =$ ____ (c) $|5 - 5| =$ ____

(d) $|-4/3| =$ ____ (e) $|a| =$ ____, if a represents the distance on the number line from the point whose coordinate is 3 to the point whose coordinate is -7.

- -

ANSWER:

(a) 3

(b) 3

(c) 0

(d) 4/3

(e) 10

- -

Some authors define absolute value of a number thus: $|0| = 0$; and if $a \neq 0$, $|a|$ is the positive member of the pair $a, -a$. You should see that this is equivalent to our definition. If $a > 0$, then a is positive, hence $|a| = a$; if $a < 0$, then $-a$ is positive and hence $|a| = -a$.

Note: $|a| = 0$ if and only if $a = 0$.

From these remarks can we conclude

(1) that $|a| \geq 0$ for every real number a?

(2) that $-|a| \leq 0$ for every real number a?

(3) that if $a \geq 0$, $|a| = a$?

- -

ANSWER:

(1) Yes.

(2) Yes.

(3) Yes.

- -

THEOREM 6.1: If a and b are real numbers then $|a \cdot b| = |a| \cdot |b|$.

To prove this theorem we note first that if either $a = 0$ or $b = 0$ then $|ab| = 0$ and $|a| \cdot |b| = 0$; thus the theorem is true in this case. If $a \neq 0$ and $b \neq 0$, we consider four cases.

I. $a > 0$, $b > 0$.

What are the other cases?

II. ____

III. ____

IV. ____

- -

ANSWER:

II. $a < 0$, $b > 0$

III. $a > 0$, $b < 0$

IV. $a < 0$, $b < 0$

- -

For Case I:

(1) If $a > 0$, $|a| = a$, and if $b > 0$, $|b| = b$, by definition of absolute value.

(2) Thus $|a| \cdot |b| = ab$

(3) Also, if $a > 0$ and $b > 0$ then $ab > 0$, by Theorem 4.10.

(4) So $|ab| = ab$, by definition of absolute value.

(5) $\therefore$ from steps (2) and (4), $|a| \cdot |b| = |ab|$.

Complete the proof for Case II below, giving order properties as reasons.

Case II:

(1) If $a < 0$, $|a| =$ ____, and if $b > 0$, $|b| =$ ____

(2) Thus $|a| \cdot |b| =$ ____. (Complete the proof)

- -

ANSWER:

(1) $-a$, b

(2) $(-a)b$ [or $-(ab)$]

(3) Also, if $a < 0$, and $b > 0$, then $ab < 0$

(4) So $|ab| = -(ab)$

(5) $\therefore |a| \cdot |b| = |ab|$

(1) Definition of absolute value

(2)

(3) Theorem 4.12

(4) Definition of absolute value

(5)

- -

For Case III the proof is the same as for Case II with the roles of a and b interchanged. Write a proof for Case IV, giving order properties as reasons. Field properties need not be given.

- -

ANSWER:

Case IV:

(1) If $a < 0$, $|a| = -a$, and if $b < 0$, $|b| = -b$

(2) Thus $|a| \cdot |b| = (-a)(-b) = ab$

(3) Also, if $a < 0$ and $b < 0$, then $ab > 0$

(4) So $|ab| = ab$

(5) $\therefore |a| \cdot |b| = |ab|$

(1) Definition of absolute value

(2)

(3) Theorem 4.11

(4) Definition of absolute value

(5)

- -

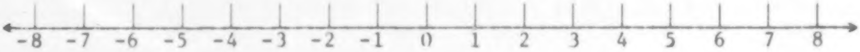
To find the solution sets for equations or inequalities such as $|x + 2| < 5$ or $|3x| \geq 10$ two additional theorems are useful. Our problem is to change a statement involving absolute value signs into one which does not involve them.

THEOREM 6.2: If a and x are real numbers and $a > 0$, then $|x| < a$ if and only if $-a < x < a$.

THEOREM 6.3: If a and x are real numbers and $a > 0$, then $|x| > a$ if and only if $x < -a$ or $a < x$.

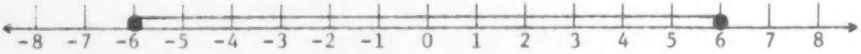
Before attempting to prove either of these theorems let us look at some numerical examples.

Consider the condition $|x| < 6$. By Theorem 6.2 any real number between ____ and ____ satisfies the condition. Show this set on the number line below.



ANSWER:

-6, 6



Note that the end points -6 and 6 are not included in this set.

Complete the following statement:

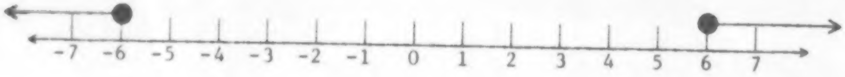
If $|x| > 6$ then, by Theorem 6.3, ____.

Show this set on the number line below:

-7
-6
-5
-4
-3
-2
-1
0
1
2
3
4
5
6
7

ANSWER:

$x < -6$ or $x > 6$.



- -

Let Theorem 6.2a be the "only if" part of Theorem 6.2, i.e.,

THEOREM 6.2a: If a and x are real numbers, $0 < a$, and $|x| < a$, then $-a < x < a$.

If you recall the definition of absolute value you see that there are three cases to investigate with respect to x, namely, Case I: $x = 0$, Case II: ____, and Case III: ____.

- -

ANSWER:

$x > 0$,

$x < 0$.

- -

If $x = 0$ then $|x| = 0$. In this case the inequalities $-a < x < a$ and $|x| < a$ clearly hold.

Complete the proof for Case II below.

Case II: $x > 0$.

(1) Since $x > 0$, $|x| =$ ____, by the definition of absolute value.

(2) By hypothesis $|x| <$ ____; hence $x <$ ____.

(3) By hypothesis $0 < a$; hence $-a < 0$. Why? (Give an order theorem or postulate). ____

(4) How can we conclude that $-a < x$? ____.

(5) From steps (4) and (2), we have $-a < x$ and $x < a$, i.e., $-a < x < a$.

- -

ANSWER:

(1) x

(2) a, a

(3) Theorem 4.5a

(4) From step (3) and the hypothesis we have $-a < 0$ and $0 < x$. By the transitive property of the order relation (Property 02) we conclude that $-a < x$.

- -

Case III. $x < 0$.

Again we must prove that $-a < x$ and that $x < a$. Write the inequality $|x| < a$ without absolute value signs; remember we are assuming $x < 0$.

- -

ANSWER:

$-x < a$, because $|x| = -x$.

- -

Complete the proof that $-a < x$ and $x < a$.

- -

ANSWER:

(1) From above, $-x < a$.

(2) By Theorem 4.7, $-x < a$ implies $-a < x$.

(3) By hypothesis $x < 0$ and $0 < a$; hence, by Property 02, $x < a$.

(4) From steps (2) and (3) we have $-a < x$ and $x < a$, i.e., $-a < x < a$.

- -

Refer to Theorem 6.2. State the "if" part of this theorem as Theorem 6.2b.

- -

ANSWER:

THEOREM 6.2b: If a and b are real numbers, $0 < a$, and $-a < x < a$, then $|x| < a$.

- -

Again there are three cases to consider: $x = 0$, $x > 0$, and $x < 0$. If $x = 0$ then clearly $-a < x < a$ and $|x| < a$ are valid. Give a proof of the theorem for Case II: $x > 0$. Note that the hypothesis $-a < x < a$ means that $-a < x$ and $x < a$. List as reasons all order properties that you use.

Case II: $x > 0$.

- -

ANSWER:

(1) By hypothesis $x > 0$; so $|x| = x$, by definition of absolute value.

(2) Also, by hypothesis, $x < a$.

(3) From steps (1) and (2) we conclude $|x| < a$.

- -

Give a proof for Case III. List as reasons all order properties used.

Case III: $x < 0$.

- -

ANSWER:

(1) By hypothesis $x < 0$; so $|x| = -x$.

(2) Also, by hypothesis, $-a < x$. Therefore, by Theorem 4.7, $-x < a$.

(3) From steps (1) and (2) we conclude $|x| < a$.

- -

THEOREM 6.3a: If a and x are real numbers, $a > 0$, and if $|x| > a$, then $x < -a$ or $a < x$.

If $a > 0$ and $|x| > a$, is $x = 0$ possible?

- -

ANSWER:

No.

Write a proof for Case II: $x > 0$ and Case III: $x < 0$, showing that in Case II, $x > a$, and in Case III, $x < -a$. List as reasons all order properties used.

Case II: $x > 0$.

Case III: $x < 0$.

ANSWER:

Case II: $x > 0$.

Since $x > 0$, $|x| = x$, by defintion of absolute value. By hypothesis, $|x| > a$. Therefore $x > a$.

Case III: $x < 0$.

Since $x < 0$, $|x| = -x$, by definition of absolute value. By hypothesis, $|x| > a$. Hence $-x > a$. Then, by Theorem 4.7, $-a > x$.

THEOREM 6.3b: If a and x are real numbers, $a > 0$, and if $x > a$ or $x < -a$, then $|x| > a$.

Prove the theorem in two parts, Part A: $x > a$, and Part B: $x < -a$. List as reasons all order properties used.

Part A: $x > a$.

ANSWER:

Part A:

(1) By hypothesis, $x > a$ and $a > 0$. Hence $x > 0$, by Property O2.

(2) Since $x > 0$, $|x| = x$ by definition of absolute value.

(3) Therefore $|x| > a$, because $x > a$.

Part B: $x < -a$.

- -

ANSWER:

Part B:

(1) Since $x < -a$, by Theorem 4.7, $a < -x$.

(2) By hypothesis, $a > 0$; hence, by Theorem 4.5, $-a < 0$.

(3) $x < -a$ and $-a < 0$ imply, by Property 02, that $x < 0$.

(4) $x < 0$ implies that $|x| = -x$, by the definition of absolute value.

(5) From steps (1) and (4) we can conclude that $|x| > a$.

- -

If a is a positive real number and x is a real number then $|x| = a$ if and only if $x = a$ or $x = -a$. This fact yields the following corollaries to Theorems 6.2 and 6.3:

1. If a and x are real numbers and $a > 0$, then $|x| \leq a$ if and only if $-a \leq x \leq a$.
2. If a and x are real numbers and $a > 0$, then $|x| \geq a$ if and only if $x \leq -a$ or $x \geq a$.

When Corollary 1 above is involved as a reason in a proof the reason will be given as simply Theorem 6.2. Similarly, when Corollary 2 is involved the reason will be given as Theorem 6.3.

We now illustrate the use of the preceding theorems in solving inequalities.

To solve the inequality $|x + 2| < 5$ we first write an equivalent statement based on Theorem 6.2, then proceed in the usual manner.

(1) $|x + 2| < 5 \Leftrightarrow -5 < x + 2 < 5$ Theorem 6.2

(2) $\Leftrightarrow$ ____

(3) Hence the solution set is ____.

- -

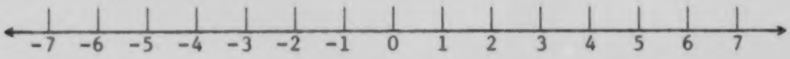
ANSWER:

(2) $-7 < x < 3$.

(3) $\{x \mid -7 < x < 3\}$.

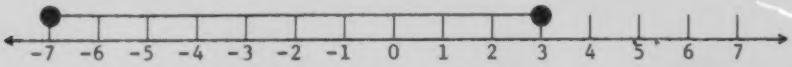
- -

Indicate the solution set $\{x \mid -7 < x < 3\}$ on the number line.



- -

ANSWER:



- -

If a and b are real numbers, then $|a - b|$ geometrically represents the distance along the number line between the points with coordinates a and b. If $a > b$ then a is $|a - b| = a - b$ units to the right of b on the line. If $a < b$ then a is $|a - b| = b - a$ units to the left of b. This remark is often useful in guessing the solution of an inequality.

The inequality in the preceding example, $|x + 2| < 5$, can be rewritten $|x - (-2)| < 5$. Hence the condition on x is that the distance from x to -2 along the number line is less than 5 units. It is gometrically clear that this condition is equivalent to $-7 < x < 3$. Hence we could guess that the solution set is $\{x \mid -7 < x < 3\}$.

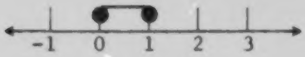
Consider the inequality $|2x - 1| \le 1$. The condition here is that the distance from $2x$ to 1 along the number line is less than or equal to 1. This is equivalent to $0 \le 2x \le 2$. Hence we can guess that the solution set is $\{x \mid 0 \le x \le 1\}$. You are now asked to verify that this is the correct solution set by using the theorems we have proved.

Solve the inequality $|2x - 1| \leq 1$. Write the steps but give a reason only for the first step. Indicate the solution set on the number line.

ANSWER:

$$
\begin{aligned}
|2x - 1| \leq 1 \quad &\Leftrightarrow \quad -1 \leq 2x - 1 \leq 1 && \text{Theorem 6.2} \\
&\Leftrightarrow \quad 0 \leq 2x \leq 2 \\
&\Leftrightarrow \quad 0 \leq x \leq 1
\end{aligned}
$$

Hence the solution set is $\{x \mid 0 \leq x \leq 1\}$.



Geometrically, in terms of distance, the inequality $4 < |3x - 2|$ states that ____.

ANSWER:

The distance from $3x$ to 2 along the number line is greater than 4.

Guess the solution set.

ANSWER:

$\{x \mid x < -2/3$ or $x > 2\}$.

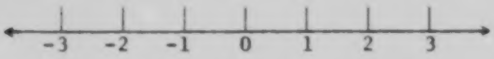
The inequality $4 < |3x - 2|$ can be solved using Theorem 6.3 as follows.

Step 1. $4 < |3x - 2|$ — $3x - 2 < -4$ or $3x - 2 > 4$ Theorem 6.3

2. $\Leftrightarrow$ ____ or ____

3. Hence the solution set is ____.

Indicate the solution set on the number line.

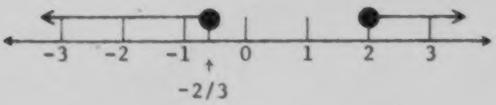


- -

ANSWER:

2. $x < -2/3$ or $x > 2$

3. $\{x \mid x < -2/3 \text{ or } x > 2\}$

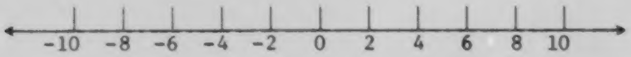


- -

Using distance considerations guess the solution set of the inequality $|1 - x| \geq 3$. ____.

Next write out a solution of the inequality using a theorem of this unit. Indicate which theorem you use.

Finally indicate the solution set on the number line.



- -

ANSWER:

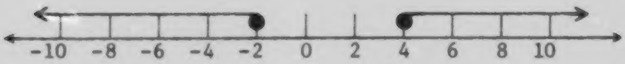
$\{x \mid x \geq 4 \text{ or } x \leq -2\}$ (Your answer should be written in set notation.)

Solution.

$|1 - x| \geq 3 \Leftrightarrow 1 - x \leq -3$ or $1 - x \geq 3$ Theorem 6.3

$\Leftrightarrow -x \leq -4$ or $-x \geq 2$

$\Leftrightarrow x \geq 4$ or $x \leq -2$



Write the solution set of $|x - 5| = 3$. Answer should be in correct set notation.

ANSWER:

$\{x \mid x = 8 \text{ or } x = 2\}$ or $\{2, 8\}$

Write the solution set of $|x - 5| < 3$.

ANSWER:

$\{x \mid 2 < x < 8\}$

Write the solution set of $|x - 5| > 3$.

ANSWER:

$\{x \mid x < 2 \text{ or } x > 8\}$

Explain why there is no real number x which is a solution of $|3x - 1| + 3 < 2$.

ANSWER:

$|3x - 1| + 3 < 2 \Leftrightarrow |3x - 1| < -1$.

But $|a| \geq 0$ for all a, by definition; therefore it is impossible to find a number x such that $|3x - 1|$ is less than -1.

Solve $5 + \left|\frac{2y - 1}{3}\right| < 6$. Show the steps in your solution in the reversible step form ($\Leftrightarrow$). You may omit the reasons. Write the solution set using set notation.

ANSWER:

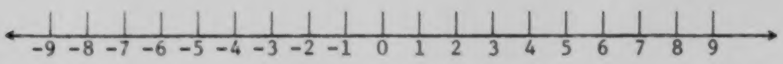
$$
\begin{aligned}
5 + \left|\frac{2y - 1}{3}\right| < 6 \quad &\Leftrightarrow \quad \left|\frac{2y - 1}{3}\right| < 1 \\
&\Leftrightarrow \quad -1 < \frac{2y - 1}{3} < 1 \\
&\Leftrightarrow \quad -3 < 2y - 1 < 3 \\
&\Leftrightarrow \quad -2 < 2y < 4 \\
&\Leftrightarrow \quad -1 < y < 2
\end{aligned}
$$

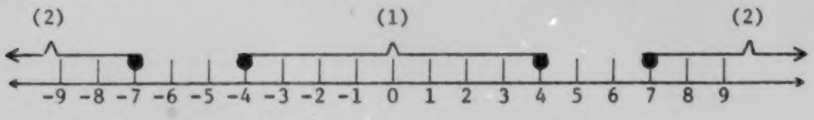
Solution set: $\{y \mid -1 < y < 2\}$.

On the number line below show the set of all numbers x which satisfy the following conditions:

(1) $|x| \leq 4$;

(2) $|x| \geq 7$.





In the usual set notation describe the set of all x which satisfy the condition $|x| \leq 4$ or $|x| \geq 7$. Do this without using absolute value signs.

ANSWER:

$\{x \mid (-4 \leq x \leq 4)$ or $(x \geq 7$ or $x \leq -7)\}$

- -

Refer to the preceding item. What are the real numbers x which satisfy the conditions $|x| \leq 4$ and $|x| \geq 7$?

- -

ANSWER:

There are none. It is impossible to satisfy simultaneously the conditions $-4 \leq x \leq 4$ and $(x \geq 7$ or $x \leq -7)$. Check this on the graph.

- -

Consider the inequality $2 < |x + 3| < 8$.

$2 < |x + 3| < 8 \iff 2 < |x + 3|$ and $|x + 3| < 8$.

$\iff [\qquad\qquad]$ and $[\qquad\qquad]$

- -

ANSWER:

$[x < -5$ or $x > -1]$ and $[-11 < x < 5]$.

- -

The two cases above are combined as follows:

$[x < -5$ and $-11 < x < 5]$ or $[x > -1$ and $-11 < x < 5]$ $\iff$

$[\qquad\qquad\qquad\qquad]$ or $[\qquad\qquad\qquad\qquad]$

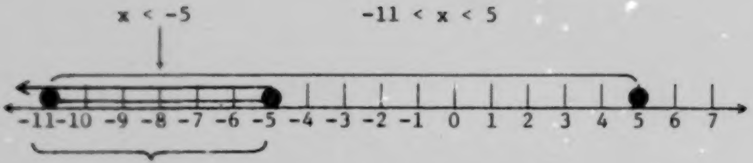
(A number line may help you to determine the answers.)

- -

ANSWER:

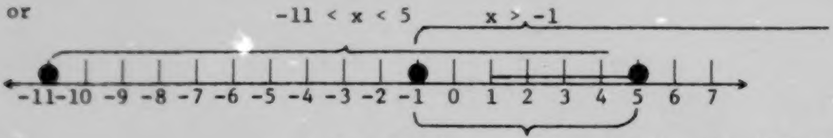
$[-11 < x < -5]$ or $[-1 < x < 5]$.

See the accompanying sketches of the various sets.

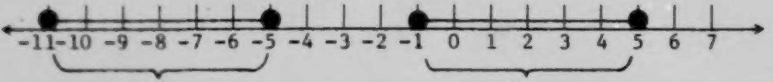

x < -5
-11 < x < 5
-11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7

$-11 < x < -5$, i.e., $x < -5$ and $-11 < x < 5$

or


-11 < x < 5
x > -1
-11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7

$-1 < x < 5$, i.e., $(-11 < x < 5)$ and $(x > -1)$


-11 -10 -9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7

$-11 < x < -5$ or $-1 < x < 5$

The complete solution to the above problem is presented below.

$$
\begin{aligned}
2 < |x+3| < 8 \quad &\Longleftrightarrow \quad 2 < |x+3| \text{ and } |x+3| < 8 \\
&\Longleftrightarrow \quad [\, x+3 < -2 \text{ or } x+3 > 2 \,] \text{ and} \\
&\qquad\ [\, -8 < x+3 < 8 \,] \\
&\Longleftrightarrow \quad [\, x < -5 \text{ or } x > -1 \,] \text{ and } [\, -11 < x < 5 \,]
\end{aligned}
$$

These cases are combined thus:

$$
\begin{aligned}
&\Longleftrightarrow \quad [\, x < -5 \text{ and } -11 < x < 5 \,] \text{ or} \\
&\qquad\ [\, x > -1 \text{ and } -11 < x < 5 \,] \\
&\Longleftrightarrow \quad [\, -11 < x < -5 \,] \text{ or } [\, -1 < x < 5 \,]
\end{aligned}
$$

Note that it is easy to guess the solution set of $2 < |x+3| < 8$, since we can interpret $|x+3|$ geometrically as the distance along the number line from x to -3. Thus the condition on x is that its distance from -3 is greater than 2 but less than 8. It is then geometrically clear that the inequality $2 < |x+3| < 8$ is equivalent to: $-11 < x < -5$ or $-1 < x < 5$.

Guess the solution set of the inequality $1 \le |x - 2| \le 5$. Write it using correct set notation.

- -

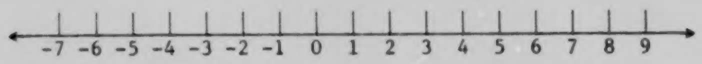
ANSWER:

$\{-3 \le x \le 1 \text{ or } 3 \le x \le 7\}$.

The condition is that the distance from x to 2 is greater than or equal to 1 but less than or equal to 5.

- -

Write out a solution of the inequality $1 \le |x - 2| \le 5$ using the theorems of this unit. You need not list reasons for steps. Use the reversible step form ($\Longleftrightarrow$). Indicate the solution set on the number line.



- -

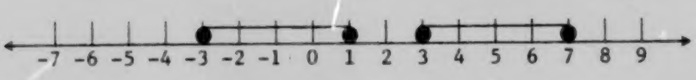
ANSWER:

$$\begin{aligned}
1 \le |x - 2| \le 5 \quad &\Longleftrightarrow \quad 1 \le |x - 2| \text{ and } |x - 2| \le 5. \\
&\Longleftrightarrow \quad [1 \le x - 2 \text{ or } -1 \ge x - 2] \text{ and} \\
&\qquad\quad [-5 \le x - 2 \le 5] \\
&\Longleftrightarrow \quad [3 \le x \text{ or } 1 \ge x] \text{ and } [-3 \le x \le 7].
\end{aligned}$$

These cases are combined thus:

$$\begin{aligned}
&\Longleftrightarrow \quad [3 \le x \text{ and } -3 \le x \le 7] \text{ or} \\
&\qquad\quad [1 \ge x \text{ and } -3 \le x \le 7] \\
&\Longleftrightarrow \quad [3 \le x \le 7] \text{ or } [-3 \le x \le 1]
\end{aligned}$$

The solution set is $\{x \mid [3 \le x \le 7] \text{ or } [-3 \le x \le 1]\}$.



- -

You know from Theorem 6.1 that $|yz| = |y| \cdot |z|$. We look now for a corresponding theorem for sums. Insert the correct relation ($=$, $<$, or $>$) in each of the following.

$|4 + 10|$ ____ $|4| + |10|$.
$|8 + (-3)|$ ____ $|8| + |-3|$.
$|(-6) + 14|$ ____ $|-6| + |14|$.
$|(-3) + (-7)|$ ____ $|-3| + |-7|$.

For any real numbers x and y, $|x + y|$ ____ $|x| + |y|$. (Guess the answer.)

- -

ANSWER:
$|4 + 10| = |4| + |10|$
$|8 + (-3)| < |8| + |-3|$
$|(-6) + 14| < |-6| + |14|$
$|(-3) + (-7)| = |-3| + |-7|$
$|x + y| \leq |x| + |y|$

This last statement is proved below.

- -

THEOREM 6.4: If x and y are real numbers, then $|x + y| \leq |x| + |y|$.

The inequality in Theorem 6.4 is sometimes referred to as "the triangle inequality".

To prove Theorem 6.4 we will prove that $|x + y|^2 \leq (|x| + |y|)^2$. Then the theorem will follow by Theorem 4.27.

PROOF: (Supply the missing reasons.)

(1) $|x + y|^2 = |(x + y)^2|$ ____
$= (x + y)^2$ ____
$= x^2 + y^2 + 2xy$

(2) $(|x| + |y|)^2 = |x|^2 + |y|^2 + 2|x| \cdot |y|$

$= |x^2| + |y^2| + 2|x| \cdot |y|$ ____

$= x^2 + y^2 + 2|x| \cdot |y|$ ____

ANSWER:

(1) Theorem 6.1 $(|x + y| \cdot |x + y| = |(x + y) \cdot (x + y)|)$

Definition of absolute value, since $(x + y)^2 \geq 0$ (Theorem 4.13).

(2) Theorem 6.1 $(|x| \cdot |x| = |x \cdot x|$, $|y| \cdot |y| = |y \cdot y|)$

Definition of absolute value, since $x^2 \geq 0$ and $y^2 \geq 0$.

We continue the proof by showing that $2xy \leq 2|x| \cdot |y|$.

(3) if $xy \geq 0$, then $|xy| = xy$ Definition of absolute value

(4) if $xy < 0$, then $|xy| =$ ____ Definition of absolute value

$-xy > 0$ Theorem 4.6

$xy < -xy$ ____

(5) from (3) and (4) we conclude that $xy \leq |xy|$

(6) $|xy| = |x| \cdot |y|$ Theorem 6.1

(7) $xy \leq |x| \cdot |y|$

(8) $2xy \leq 2|x| \cdot |y|$ 04

ANSWER:

(4) $-xy$

02

Complete the proof.

ANSWER:

(8) $2xy \leq 2|x| \cdot |y|$

(9) $x^2 + y^2 + 2xy \leq x^2 + y^2 + 2|x| \cdot |y|$ 03

(10) $|x + y|^2 \leq (|x| + |y|)^2$

(11) $|x + y| \leq |x| + |y|$ Theorem 4.27

REVIEW ITEMS

1. Prove: If $|x| = 0$, then $x = 0$.

List as reason each order property that you use, but do not list field properties.

ANSWER:

PROOF: By 01, either $x = 0$, $x > 0$, or $x < 0$. The proof consists of showing that $x > 0$ and $x < 0$ are impossible:

Suppose $x > 0$. Then $|x| = x$, by definition of absolute value. Hence $|x| > 0$. Since, by hypothesis, $|x| = 0$, it cannot be true that $|x| > 0$ (by 01). Hence $x > 0$ is impossible.

Suppose $x < 0$. Then $|x| = -x$, by definition of absolute value. Also, $-x > 0$, by Theorem 4.6. Thus $|x| > 0$. Again (by 01) this cannot be true; so $x < 0$ is impossible.

---

2. Let b be a non-zero real number. Prove that $|b| \cdot \left|\frac{1}{b}\right| = 1$. List as reason any theorem you use from this unit.

ANSWER:

Since $1 > 0$, $|1| = 1$ by definition of absolute value. Then $|b/b| = |1| = 1$. But $|b/b| = |b \cdot 1/b| = |b| \cdot |1/b|$, by Theorem 6.1. Therefore $|b| \cdot |1/b| = 1$.

Since $|b| \cdot |1/b| = 1$, $|1/b| = 1/|b|$, for each non-zero real number b. Using this fact prove that $|a/b| = |a|/|b|$ for real numbers a and b with $b \neq 0$. List as reason any theorem you use from this unit.

ANSWER:

$|a/b| = |a \cdot 1/b| = |a| \cdot |1/b|$, by Theorem 6.1. But by the above, $|1/b| = 1/|b|$. Therefore $|a/b| = |a| \cdot |1/b| = |a| \cdot 1/|b| = |a|/|b|$.

---

3. Find the solution set for the inequality $18 - 2|y + 3| \geq 12$. Show your work. No reasons are required.

ANSWER:

$$
\begin{aligned}
18 - 2|y + 3| \geq 12 &\iff 6 \geq 2|y + 3| \\
&\iff 3 \geq |y + 3| \\
&\iff -3 \leq y + 3 \leq 3 \\
&\iff -6 \leq y \leq 0
\end{aligned}
$$

$\therefore$ Solution set is $\{y \mid -6 \leq y \leq 0\}$.

---

4. Give the solution set for

(1) $|x|/x < 2$

(2) $|x| \geq x$

(3) $-3|x| + 3 < 3$

ANSWER:

(1) $\{x \mid x \neq 0\}$

(2) The set of all real numbers

(3) $\{x \mid x \neq 0\}$

---

5. Prove: If x and y are real numbers, then

$|x - y| \geq |x| - |y|$.

List as reason(s) any theorems that you use from this unit.

[Hint: Write $x = (x - y) + y$]

ANSWER:

PROOF:

$|x| = |(x - y) + y| \leq |x - y| + |y|$ Theorem 6.4

$\therefore |x| - |y| \leq |x - y|$

COMPLETENESS OF THE REAL NUMBER SYSTEM

The real number system is not the only ordered field. For example, the system of rational numbers is also a field having the properties 01, 02, 03, and 04. But the system of real numbers has an additional property called completeness which the set of rational numbers does not have. We say that the real number system is a complete ordered field.

Before we can state this property it is necessary to define two new terms, upper bound and least upper bound. Consider the set A = {1, 1.4, 1.41, 1.414, ...} obtained by taking successive finite decimal approximations for $\sqrt{2}$. This set A is a subset of B = $\{x \mid x$ is a real number and $x^2 < 2\}$. Each of these sets contains numbers which are less than $\sqrt{2}$ and neither has a member which is greater than $\sqrt{2}$. Then it would seem that $\sqrt{2}$ could be called an upper bound for the set A or for the set B. By this same reasoning, would you call 3 an upper bound? ____ 2.5? ____ 10? ____ 1.4? ____

- -

ANSWER:

Yes

Yes

Yes

No

- -

DEFINITION 7.1: A number u is called an upper bound of a non-empty set S of real numbers if $u \geq x$ for each element x in S.

Let S be the set of all negative real numbers.

Is 3 an upper bound of S?
Is 0 an upper bound of S?
Is -1 an upper bound of S?

- -

ANSWER:

Yes.
Yes.
No.

- -

If $B = \{x \mid 3 \leq x \leq 12,$ and x is a real number$\}$, which of the following are upper bounds for the set B? 12, 15, 3, 12.1, 11.9.

- -

ANSWER:

12, 15, 12.1

- -

Give an upper bound for the set $S = \{x \mid x > 2,\ x$ is a real number$\}$.

- -

ANSWER:

There is no upper bound for this set.

- -

DEFINITION 7.2: A real number v is called the least upper bound (l.u.b.) of S if

(a) v is an upper bound of S,
(b) for every upper bound u of S, $v \leq u$.

For an upper bound of the finite set $S = \{3, 6, 9, 12, 15, 18\}$ we could choose the number ____ or any larger number.

The least upper bound of the set S is ____.

Is the number you have selected as the l.u.b. an element of S? ____.

ANSWER:

18

18

Yes. (If your answer was correct.)

Consider the infinite sets

(1) $S = \{1/2, 2/3, 3/4, \ldots, \frac{n}{n+1}, \ldots\} = \{\frac{n}{n+1} \mid n$ is a natural number$\}$

(2) $T = \{2/1, 3/2, 4/3, \ldots, \frac{n+1}{n}, \ldots\} = \{\frac{n+1}{n} \mid n$ is a natural number$\}$

Find the least upper bound of each set. Is the number you have selected in each case in the given set?

ANSWER:

(1) 1; no, $\frac{n}{n+1} < 1$ for each natural number n.

(2) 2; yes.

If S is a set of real numbers and b is a number in S such that $b \geq x$ for every number x in S then b is the largest number in S. If S has a largest element b then b is the l.u.b. of S. b is an upper bound because $b \geq x$ for every number x in S; and if u is any upper bound, $u \geq b$ because b is in S. However, a set S may have a l.u.b. without having a largest element; then the l.u.b. of S is not an element of S. The example

$S = \{\frac{n}{n+1} \mid n$ is a natural number$\}$

given above has l.u.b. 1 but 1 is not in the set S. Hence S has a l.u.b. but does not have a largest element.

Let $S = \{x \mid 0 < x < 1,\ x$ is a real number$\}$.

(a) What is the l.u.b. of S? ____

(b) Does S have a largest element? ____

ANSWER:

(a) 1

(b) No.

Let $S = \{x \mid 0 \leq x \leq 1,\ x$ a real number$\}$.

(a) What is the l.u.b. of S? ____

(b) Does S have a largest element? ____

ANSWER:

(a) 1

(b) Yes

Find the least upper bound of each of the sets listed below. Is the least upper bound an element of the given set?

(1) $S = \{1/2, 1/3, 1/4, \ldots, \frac{1}{n+1}, \ldots\} = \{\frac{1}{n+1} \mid n$ is a natural number$\}$

(2) $T = \{-1/2, -1/3, -1/4, \ldots, -\frac{1}{n+1}, \ldots\} = \{-\frac{1}{n+1} \mid n$ is a natural number$\}$

ANSWER:

(1) 1/2; yes.

(2) 0; no, $-\frac{1}{n+1} < 0$ for each natural number n.

- -

We will now give our final postulate for the system of real numbers.

COMPLETENESS PROPERTY: Every non-empty set of real numbers which has an upper bound also has a least upper bound.

Our complete set of axioms, or postulates, for the system of real numbers consists of the field properties A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, M_{in}, the order properties 01, 02, 03, and 04, and the Completeness Property stated above. The Completeness Property is the only one of these which is not ordinarily studied (in some form) in high school algebra. However, it is basic to the theory of limits which underlies calculus.

THEOREM 7.1: If a subset S of R has a least upper bound, then it has only one.

To prove Theorem 7.1 we suppose that v and w are least upper bounds of S. We need to prove that ____.

- -

ANSWER:

$v = w$

- -

If $v \neq w$ then we must have either ____ or ____.

- -

ANSWER:

$$\left.\begin{matrix} v < w \\ v > w \end{matrix}\right\} \quad \text{or} \quad \left\{\begin{matrix} v > w \\ v < w \end{matrix}\right.$$

- -

Let us show that $v < w$ is not possible. Since w is a l.u.b. of S, we must have $w \leq u$ for every upper bound u. But v is an upper bound. So $w \leq v$. This implies that $v < w$ is impossible, by O1. Similar reasoning shows that $w < v$ is impossible. Therefore $v = w$, and the theorem is proved.

We have stated the Completeness Property in terms of upper bounds and the least upper bound of a non-empty set of real numbers. This property can also be stated in terms of lower bounds and the greatest lower bound, if suitable definitions are given for these terms. Complete each of the following, by analogy with Definitions 7.1 and 7.2.

(1) DEFINITION 7.3: A number b is called a lower bound of a non-empty set S of real numbers if ____.

(2) DEFINITION 7.4: A number c is called the greatest lower bound (g.l.b.) of S if ____.

(3) COMPLETENESS PROPERTY:

ANSWER:

(1) $b \leq x$ for each element x of S.

(2) c is a lower bound of S, and for every lower bound b of S, $c \geq b$.

(3) Every non-empty set S of real numbers which has a lower bound has a greatest lower bound.

A proof similar to that used in proving Theorem 7.1 can be given to prove the following theorem.

THEOREM 7.2: If a subset S of R has a greatest lower bound, then it has only one.

Let S be the set of all negative real numbers.

(a) Does S have a lower bound? ____

(b) Does S have a greatest lower bound? ____

ANSWER:

(a) no.

(b) no.

Let $S = \{x \mid 3 \le x \le 12,\ x \text{ a real number}\}$. Which of the following are lower bounds for the set S? 2, 3, 10/3, -13, 12.

ANSWER:

2, 3, -13

Consider the following statements about a set S.

(1) S has no upper bound.

(2) S has no lower bound.

(3) S has a least upper bound which is not in the set S.

(4) S has a greatest lower bound which is not in the set S.

(5) S has a least upper bound which is in the set S.

(6) S has a greatest lower bound which is in the set S.

For each of the following sets S indicate which of the above six statements are true for S

(a) S = the set of all integers.

(b) $S = \{x \mid -5 \le x \le 1/2,\ x \text{ a real number}\}$.

(c) $S = \{x \mid -5 < x \le 1/2,\ x \text{ a rational number}\}$

(d) S = the set of all positive real numbers.

ANSWER:

(a) (1), (2)

(b) (5), (6)

(c) (4), (5)

(d) (1), (4)

Let S be a non-empty set of real numbers which has a lower bound. We define a new set T to be the set of all lower bounds of S. Thus, T is a non-empty set and, by the definition of lower bound of S, a real number b is in T if and only if ____ for every number x in S.

ANSWER:

$b \leq x$.

Therefore, for any element x in S and any element b in T, $b \leq x$.

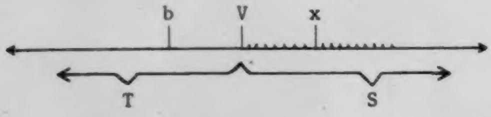
Does the set T have an upper bound? Explain.

ANSWER:

Yes, every element of S is an upper bound of T.

If we assume the Completeness Property stated in terms of upper bounds we can prove the Completeness Property stated in terms of lower bounds. The proof is outlined below.

We assume that S is a non-empty set which has a lower bound and show that S has a greatest lower bound. As above, we let T be the set of all lower bounds of S. Then every element of T is a lower bound of S and every element of S is an upper bound of T. The following diagram may prove helpful.



T is a non-empty set of real numbers. If x is any element of S, then x is an upper bound of T. Since we are assuming the Completeness Property stated in terms of upper bounds, we can say that T has ____.

- -

ANSWER:

a least upper bound.

- -

Denote the least upper bound of T by v. We wish to show that v is the greatest lower bound of S. To do this we must show

(a)

(b)

- -

ANSWER:

(a) v is a lower bound of S.

(b) If b is any lower bound of S then $b \leq v$.

- -

If b is any lower bound of S, then b is in what set?

- -

ANSWER:

T.

- -

Why can we conclude that $b \leq v$?

- -

ANSWER:

b is in T and v is an upper bound of T. Therefore $b \leq v$.

- -

Thus statement (b) is true. Now we prove statement (a). If x is any element of S we have seen that x is an upper bound of T.

But v is the least upper bound of T. Therefore we must have the inequality ____ for every element x of S.

ANSWER:

$v \leq x$.

But this just says that v is a lower bound of S, which is statement (a).

We have proved that the Completeness Property stated in terms of upper bounds implies the Completeness Property stated in terms of lower bounds. We could also prove the converse of this statement: the Completeness Property stated in terms of lower bounds implies the Completeness Property stated in terms of upper bounds. Therefore the Completeness Property may be stated in terms of either upper or lower bounds.

What is the greatest lower bound of the set of all real numbers of the form

$\dfrac{x^2 - 1}{x - 1}$ with $x > 1$?

ANSWER:

g.l.b. = 2.

If $x > 1$, then $\dfrac{x^2 - 1}{x - 1} = \dfrac{(x + 1)(x - 1)}{x - 1} = x + 1$.

Find the products:

$(x - 1)(x + 1) =$ ____

$(x - 1)(x^2 + x + 1) =$ ____

$(x - 1)(x^3 + x^2 + x + 1) =$ ____

Generalize: $(x - 1)(x^n + x^{n-1} + \ldots + x + 1) =$ ____

- -

ANSWER:

$x^2 - 1$.

$x^3 - 1$.

$x^4 - 1$.

$x^{n+1} - 1$.

- -

What is the greatest lower bound of the set of all real numbers $\frac{x^3 - 1}{x - 1}$ with $x > 1$?

- -

ANSWER:

g.l.b. = 3.

From the preceding problem, if $x > 1$ then

$$\frac{x^3 - 1}{x - 1} = \frac{(x^2 + x + 1)(x - 1)}{x - 1} = x^2 + x + 1$$

Hence 3 is the greatest lower bound.

- -

What is the greatest lower bound of the set of real numbers $\frac{x^4 - 1}{x - 1}$ with $x > 1$?

- -

ANSWER:

4

- -

What is the greatest lower bound of the set of real numbers $\frac{x^n - 1}{x - 1}$ with $x > 1$?

- -

ANSWER:

n

Find the least upper bound of the set of real numbers $\frac{x^2 - 1}{x - 1}$ with $x < 1$.

ANSWER:

l.u.b. $= 2$.

Find the least upper bound of the set of real numbers $\frac{x^3 - 1}{x - 1}$ with $0 < x < 1$.

ANSWER:

l.u.b. $= 3$.

Could you give a least upper bound for the set of real numbers $\frac{x^3 - 1}{x - 1}$, for all x such that $x < 1$? Explain.

ANSWER:

No, there is no upper bound for the set, hence no least upper bound.

DECIMAL EXPANSIONS

You are probably familiar with the statement that every positive real number has a finite or infinite decimal expansion and that this expansion is unique if we do not allow expansions which end in an infinitely repeated succession of 9's. It is our purpose here to take a closer look at the meaning of this statement.

The expansion 237.51 represents the number

$2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0 + 5 \cdot 10^{-1} + 1 \cdot 10^{-2}$.

The expansion 3025.004 represents what number?

ANSWER:

$3 \cdot 10^3 + 2 \cdot 10^1 + 5 \cdot 10^0 + 4 \cdot 10^{-3}$

Every finite decimal represents a number as a finite sum of multiples, $a \cdot 10^n$, of powers of 10 where a is a non-negative integer less than 10 and n is an integer -- positive, negative, or zero. But we cannot add an infinite number of terms. Therefore, in what sense is it true that $1/3 = .3333 \ldots$? We can give an answer to this question using the notion of least upper bound. Consider the set S consisting of the numbers: .3, .33, .333, .3333, ... The set S is infinite but each number in S has a finite decimal expansion. It can be shown, although we will not do so, that the l.u.b. of the set S is the number $1/3$. In a similar way we can associate with any positive infinite decimal a set S of numbers which have finite expansions. This set will have a l.u.b. and we say that the given infinite decimal is the expansion of the number which is the l.u.b. of S.

We will not give proofs here but the following statements are true.

(1) Every positive number has a finite or infinite decimal expansion.

(2) If we do not allow expansions which end in an infinitely repeated succession of 9's, then the decimal expansion of each positive number is unique.

Find a finite decimal expansion with which it would be reasonable to associate the number represented by 2.379999 ... (ending in an infinitely repeated succession of 9's).

ANSWER:

2.38

Consider two infinite decimal expansions whose first five digits are given as follows: .13275... and .13268... For purposes of this exercise it does not matter what the remaining digits are. The first decimal represents the l.u.b. of the set $S_1 = \{.1, .13, .132, .1327, \ldots\}$, and the second decimal represents the l.u.b. of the set $S_2 = \{.1, .13, .132, .1326, \ldots\}$. Find an upper bound of S_2 which is not an upper bound of S_1. Why does this show that the second decimal represents a smaller number than the first decimal?

ANSWER:

Any number greater than or equal to .1327 and less than .13275 will be an upper bound for S_2 but not an upper bound for S_1; e.g., .1327 itself. Since the l.u.b. of S_2 is less than the l.u.b. of S_1, the second decimal represents a smaller number than the first.

Since many high school algebra books "define" a real number to be a finite or infinite decimal expansion, it is perhaps worth pointing out that it is very difficult to give a satisfactory development of the real numbers from this definition without using the least upper bound notion or limits in some form. Even the definitions of addition and multiplication pose some difficulties. You might ask yourself how one should define as finite or infinite decimals the numbers $a + b$ and $a \cdot b$, where

$a = .86866866686666\ldots$ and $b = .235233523335\ldots$,

(The expansions of a and b continue the pattern suggested in the terms given.)

REVIEW ITEMS

1. What is the least upper bound of each of the following sets?

(a) $\{x \mid 0 < x < 3/2\}$

(b) set of non-positive real numbers

(c) set of negative integers

(d) set of all even integers

- -

ANSWER:

(a) 3/2

(b) 0

(c) -1

(d) no least upper bound

- -

2. In which of the sets of Item 1 is the l.u.b. an element of the set?

- -

ANSWER:

(b) and (c)

- -

3. Let $S = \{\frac{2n}{n+1} \mid n$ is a natural number$\}$. What is the l.u.b. and the g.l.b. of S?

- -

ANSWER:

l.u.b. $S = 2$

g.l.b. $S = 1$

- -

4. Find a set of rational numbers whose l.u.b. is represented by the infinite decimal

.232332333233332...

(The pattern indicated is continued.)

ANSWER:

S = {.2, .23, .232, .2323, .23233, ...}.

---

5. Does it make sense to talk about the l.u.b. of the decimal .232332333233332...?

ANSWER:

No. The decimal represents a single number, not a set of numbers. The number represented by the decimal is the l.u.b. of the set of rational numbers which are the finite decimal approximations to the given infinite decimal (as given in Item 4).

VIII. NATURAL NUMBERS

INTRODUCTION

The set N of *natural numbers*, or *positive integers*, is an important subset of the set of real numbers. Natural numbers are often called *counting numbers* since they are the numbers used in counting. When a child begins the study of arithmetic he begins with these numbers.

It is possible to give a definition of the set of natural numbers based on properties of sets. When this is done one can construct successively the set of the integers, the set of rational numbers, and the set of real numbers. However, since we already have a set of axioms for the system of real numbers, it is more suitable for our purposes to give a definition in terms of real numbers.

If you were asked to give a definition of the set of natural numbers, you might well answer, "the set consisting of the number 1 and all numbers obtained from 1 by successively adding 1". The definition which we give is a precise statement of this basic idea.

DEFINITION OF THE SET OF NATURAL NUMBERS

DEFINITION 8.1: The *set of natural numbers* is a subset of the set of real numbers having the following properties:

(a) 1 is a natural number.

(b) If n is a natural number, then $n + 1$ is a natural number.

(c) If n is a natural number, then $n \geq 1$.

(d) If n is a natural number, then there is no natural number between n and $n + 1$; i.e., for no natural number m is it true that

$n < m$ and $m < n + 1$.

Note that in stating Definition 8.1 we are in effect stating (a), (b), (c), and (d) as postulates for the set of natural numbers. We will refer to these as Postulate (a), Postulate (b), etc.

We will need to show later that Definition 8.1 uniquely defines the set of natural numbers, i.e., that there cannot be two different subsets of the real numbers for which Postulates (a) - (d) are valid.

The many familiar properties of the natural numbers can be derived from Postulates (a) - (d) and the postulates for the real numbers. For example, we can prove the following theorem.

THEOREM 8.1: If n is a natural number and $n \neq 1$, then $n - 1$ is a natural number.

In proving this theorem we will make use of the Completeness Property of the real numbers.

PROOF: Assume that there is a natural number k such that $k \neq 1$ and such that $k - 1$ is not a natural number. We wish to show that this assumption leads to a contradiction. Let S be the set of all natural numbers less than k. We know that S is not empty because, by Postulates (a) and (c), ____ is in S.

- -

ANSWER:

1.

- -

The number ____ is an upper bound for the set S. Hence, by the Completeness Property, S has a ____.

- -

ANSWER:

k

least upper bound (in the set of real numbers).

- -

Denote the least upper bound of S by $\bar{s}$. Is $\bar{s} - 1$ an upper bound for S? Why?

ANSWER:
No; $\bar{s} - 1$ is less than $\bar{s}$, the least upper bound for S.

Since $\bar{s} - 1$ is not an upper bound for S we know that there is an element s in S such that ____.

ANSWER:
$\bar{s} - 1 < s$

Therefore $\bar{s} < s + 1$, by O3 and Theorem 4.13. Is $s + 1$ a natural number? Why?

ANSWER:

Yes; s is a natural number because it is in S; therefore $s + 1$ is a natural number, by Postulate (b).

Is $s + 1$ in S? Why?

ANSWER:
No; $s + 1 > \bar{s}$ and $\bar{s}$ is an upper bound for S.

Since $s + 1$ is a natural number not in S what can we say about the relative order of $s + 1$ and k?

ANSWER:

$s + 1 \geq k$, because S is the set of all natural numbers which are less than k.

- -

Therefore $s < k \leq s + 1$. Why can we conclude that $k = s + 1$?

- -

ANSWER:

Postulate (d) says there is no natural number between s and $s + 1$. Since k is a natural number and $s < k \leq s + 1$, we must have $k = s + 1$

- -

How does $k = s + 1$ lead to a contradiction of the assumption that $k - 1$ is not a natural number?

- -

ANSWER:

If $k = s + 1$, then $k - 1 = s$. We know that s is a natural number.

- -

Now reconstruct the entire proof of Theorem 8.1. (You may review the preceding items first, but once you begin to write the proof do not look back.)

- -

ANSWER:

Theorem 8.1: If n is a natural number and $n \neq 1$, then $n - 1$ is a natural number.

PROOF: Assume that k is a natural number such that $k \neq 1$ and that $k - 1$ is not a natural number. Let S be the set of all natural numbers less than k. $k \neq 1$, $k > 1$, by Postulate (c); therefore 1 is in S. k is an upper bound for S; therefore, by the Completeness Property of the real numbers, S has a least upper bound $\bar{s}$. $\bar{s} - 1$ is less than $\bar{s}$, the least upper bound for S, so there is a natural number s in S such that $\bar{s} - 1 < s$. Then $\bar{s} < s + 1$. $s + 1$ is a natural number by Postulate (b); and $s + 1$ is not in S because $s + 1 > \bar{s}$. Therefore $s + 1 \geq k$. We have $s < k \leq s + 1$. By Postulate (d), $k = s + 1$. This shows that $k - 1 = s$ and contradicts the assumption that $k - 1$ is not a natural number. Thus the theorem is true.

It is perhaps worth pointing out here that the Completeness Postulate is essential for the proof of Theorem 8.1. It is possible to construct an ordered field which satisfies all the other postulates for the real number system (i.e., all except the Completeness Postulate) and which has a subset N satisfying Postulates (a) - (d) but for which Theorem 8.1 fails to hold. Such an example is too difficult to be given here.

WELL-ORDERING AND MATHEMATICAL INDUCTION

The set of natural numbers has a very important property which is not possessed by the set of integers, the set of rational numbers, and the set of real numbers. We refer to it as the Well-ordering Property.

DEFINITION 8.2: A non-empty set S of real numbers is well-ordered provided that every non-empty subset of S contains a least element.

Read the preceding definition carefully, then answer the following items.

If S is a well-ordered set does S have a least element?

ANSWER:

Yes, because S is a non-empty subset of itself.

- -

If S is a set of real numbers which has a least element, is S well-ordered?

- -

ANSWER:

Not necessarily. As an example, consider the set S of non-negative real numbers. The set S has a least element, viz. 0. But the set T of positive real numbers, which is a non-empty subset of S, does not have a least element; hence S is not well-ordered. The definition says that not only does S itself have a least element but every non-empty subset of S also contains a least element.

- -

Let S be the set of non-negative rational numbers.

Does S have a least element?

Is S a well-ordered set?

- -

ANSWER:

Yes, zero is the least element of S.

No, S is not well-ordered; e.g., the positive rational numbers form a subset of S without a least number.

- -

Which of the following sets are well-ordered? (Answer on the basis of your experience with the given sets.)

(a) Set of integers.

(b) Set of even natural numbers.

(c) Set of positive rational numbers with numerator 3.

(d) Set of positive rational numbers with denominator 2.

ANSWER:

(b) and (d).

(In (a), the set of integers itself does not contain a least element. In (c), the set of positive rational numbers with numerator 3 does not contain a least element.)

THEOREM 8.2: The set N of natural numbers is well ordered.

What must we prove in order to establish the truth of Theorem 8.2?

ANSWER:

We must prove that every non-empty subset of N has a least element.

What postulates for N tell us that 1 is the least element of N?

ANSWER:

Postulates (a) and (c).

Let S be any non-empty set of natural numbers. The number 1 is a lower bound for S. Why?

ANSWER:

Postulate (c).

Then, by the Completeness Property stated in terms of lower bounds, the set S has a ____.

ANSWER:

greatest lower bound (g.l.b.)

Let $\bar{s}$ be the g.l.b. of S. If $\bar{s}$ is in S then it is the least element of S, because no element of S can be less than the g.l.b. of S. We have seen in Unit VII that the g.l.b. of a set of real numbers does not have to be in the set. So we must prove that in the case which we are considering here, $\bar{s}$ is in S.

Suppose $\bar{s}$ is not in S. We will show that this leads to a contradiction; then the theorem will be proved.

(1) There exists an element s_1 in S such that $s_1 < \bar{s} + 1$. Why?

ANSWER:

Because $\bar{s}$ is the g.l.b. of S and $\bar{s} + 1 > \bar{s}$; i.e., $\bar{s} + 1$ is not a lower bound of S.

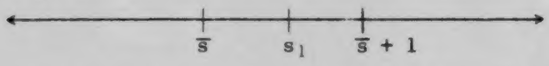
---

(2) $\bar{s} < s_1$. Why?

ANSWER:

Definition of g.l.b. and our assumption $\bar{s}$ is not in S. Thus every element of S is greater than $\bar{s}$, no element of S is equal to $\bar{s}$.

The following geometrical picture may be helpful.



(3) There is an element s_2 in S such that $s_2 < s_1$. Why?

ANSWER:

Because $\bar{s}$ is the g.l.b. of S and $s_1 > \bar{s}$; i.e., s_1 is not a lower bound of S.

---

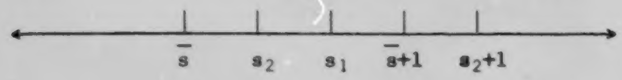
(4) $\bar{s} < s_2$. Why?

ANSWER:

Definition of g.l.b. and our assumption that $\bar{s}$ is not in S.

From (4) $s_2 > \bar{s}$, we obtain

(5) $s_2 + 1 > \bar{s} + 1$.



Bringing all our inequalities together, we have, from our assumption that $\bar{s}$ is not in S,

(1) $s_1 < \bar{s} + 1$.
(2) $\bar{s} < s_1$.
(3) $s_2 < s_1$.
(4) $\bar{s} < s_2$.
(5) $s_2 + 1 > \bar{s} + 1$.

What inequality do statements (5) and (1) imply?

ANSWER:

(6) $s_2 + 1 > s_1$

Explain why statements (3) and (6) lead to a contradiction.

- -

ANSWER:

(3) and (6) state that the natural number s_1 is between the two natural numbers s_2 and $s_2 + 1$. This contradicts Postulate (d).

- -

Since our assumption that $\bar{s}$, the g.l.b. of S, is not in S leads to a contradiction, it must be true that $\bar{s}$ is in S. We have shown that each non-empty subset of N has a least element, namely the g.l.b. of the set. Hence N is ____.

- -

ANSWER:

well-ordered.

- -

Reconstruct the proof of Theorem 8.2. Do not look back over the preceding items after you have begun to write the proof.

- -

ANSWER:

THEOREM 8.2: The set N of natural numbers is well-ordered.

We want to show that every non-empty subset S of N has a least element. By Postulates (a) and (c), we know that N has the least element 1.

PROOF: Let S be any non-empty set of natural numbers. Be definition of lower bound and Postulate (c), 1 is a lower bound of S. Thus, by the Completeness Property stated in terms of lower bounds, the set S has a greatest lower bound (g.l.b.).

Let $\bar{s}$ be the g.l.b. of S. If $\bar{s}$ is in S then S has a least element, viz., $\bar{s}$.

Suppose $\bar{s}$ is not in S. We wish to show that this leads to a contradiction.

Since $\bar{s}$ is the g.l.b. of S and $\bar{s} + 1 > \bar{s}$, there exists an element s_1 in S such that,

(1) $s_1 < \bar{s} + 1$.

(2) $\bar{s} < s_1$, by definition of g.l.b. and our assumption that $\bar{s}$ is not in S. There is an element s_2 in S such that

(3) $s_2 < s_1$, because $\bar{s}$ is the g.l.b. of S and $s_1 > \bar{s}$.

(4) $\bar{s} < s_2$, by definition of g.l.b. and our assumption that $\bar{s}$ is not in S. From (4) we have

(5) $s_2 + 1 > \bar{s} + 1$. From (5) and (1),

(6) $s_2 + 1 > s_1$. From (3) and (6),

(7) $s_2 < s_1 < s_2 + 1$.

We have reached a contradiction to Postulate (d). Hence $\bar{s}$ is in S, and every non-empty subset of N has a least element, namely the g.l.b. of the set. Therefore N is well-ordered.

The Well-ordering Property of the natural numbers is one of the most powerful tools for constructing proofs in all mathematics. Proofs which depend upon this property arise so often that they have been given a special name. Any proof in mathematics which is based on the Well-ordering Property of the natural numbers is called a proof by mathematical induction.

Many proofs by mathematical induction are not based directly upon well-ordering but upon the following principle which can be proved using the Well-ordering Property.

THEOREM 8.3: (Induction Principle) If S is a subset of N such that

(a) 1 is in S, and

(b) if k is any number in S, then k + 1 is also in S, then S is all of N.

If a set S satisfies (a) and (b) of the theorem, then 1 is in S. Then by (b), taking $k = 1$, $1 + 1 = 2$ is in S. Again by (b), taking $k = 2$, $2 + 1 = 3$ is in S. It is intuitively clear that this procedure can be continued to conclude that every natural number is in S.

We will give a proof of the Induction Principle using the Well-ordering Property.

PROOF: We assume that S is a subset of N which satisfies (a) and (b) above.

If $S \neq N$, then there is at least one natural number which is not in S.

Let T be the set of all natural numbers not in S. Then T is a non-empty subset of N, and S and T have no element in common. Furthermore, we can say that T has a smallest element, t. Why?

- -

ANSWER:

By the Well-ordering Property.

- -

In addition we can say that $t \neq 1$. Why?

- -

ANSWER:

1 is in S by statement (a) above. Hence 1 is not in T.

- -

Since $t \neq 1$, Theorem 8.1 tells us that $t - 1$ is a natural number. Is $t - 1$ in S or in T?

- -

ANSWER:

$t - 1$ is in S. Since $t - 1 < t$ and t is the smallest number in T, then $t - 1$ is in S.

If k is in S, is $k + 1$ in S or in T?

ANSWER:

$k + 1$ is in S by statement (b) of the hypothesis.

Since $t - 1$ is in S, let $k = t - 1$. Then $k + 1 =$ ____.

ANSWER:

t.

The assumption $S \neq N$ has led to a contradiction. What is it?

ANSWER:

t is in S and t is not in S.

Therefore, $S = N$

We will use the Induction Principle in proving the next two theorems. These provide excellent illustrations of proofs by mathematical induction.

THEOREM 8.4: The set of natural numbers is closed under addition.

PROOF: Let m be an arbitrary natural number. We will show by mathematical induction that $m + n$ is a natural number for every natural number n. Let S be the set of all natural numbers n such that $m + n$ is a natural number. (We emphasize that, in this discussion, m is a fixed natural number.)

(1) 1 is in S, i.e., $m + 1$ is a natural number. Why?

ANSWER:

Postulate (b) for the natural numbers.

---

(2) Assume k is in S, i.e., $m + k$ is a natural number.

(3) Prove $k + 1$ is in S.

ANSWER:

(3) $m + (k + 1) = (m + k) + 1$. By our assumption (2), $m + k$ is a natural number, and by Postulate (b), $(m + k) + 1$ is a natural number; hence $k + 1$ is in S.

Therefore $S = N$, by the Induction Principle, and the proof is complete.

THEOREM 8.5: The set of natural numbers is closed under multiplication.

What must be shown in order to prove Theorem 8.5?

ANSWER:

That if m is a natural number, then $m \cdot n$ is a natural number for each natural number n.

Let m be a natural number and let S be the set of all natural numbers n such that $m \cdot n$ is a natural number. Prove that $S = N$.

Hint: You will need to use Theorem 8.4 in your proof.

ANSWER:

(1) 1 is in S because $m \cdot 1 = m$.

(2) Assume k is in S, i.e., $m \cdot k$ is a natural number.

(3) $m \cdot (k + 1) = m \cdot k + m \cdot 1 = m \cdot k + m$ is a natural number by step (2) and Theorem 8.4. Hence $k + 1$ is in S if k is in S.

$\therefore S = N$, by the Induction Principle.

- -

The two preceding theorems tell us that addition and multiplication are closed operations in the set of natural numbers. The set N of natural numbers together with these two operations is then an algebraic system. It is natural to ask which of the field postulates are valid for the system N.

If you will study carefully the field postulates given for the real numbers in Unit II, you will see that there is an essential difference between Postulates A_a, A_c, M_a, M_c, and D on the one hand and A_{id}, A_{in}, M_{id}, and M_{in} on the other. Each of the former postulates gives an equality which must hold in general for real numbers, while each of the latter postulates states the existence of a special real number or of special real numbers.

Each of the Postulates A_a, A_c, M_a, M_c, and D is valid for N because every natural number is also a real number. For example, if a and b are natural numbers then a and b are also real numbers; therefore $a + b = b + a$ by Property A_c for real numbers. Therefore Property A_c is valid for N. However, in testing Postulates A_{id}, A_{in}, M_{id}, and M_{in} for N we have to determine if the special element (or elements) which is stated to exist in the set of real numbers is also in the set N. For example, A_{id} states the existence of an additive identity 0. But the real number 0 is not a natural number. The set N does not contain an identity element for addition. So A_{id} is not valid for N.

Which of the Properties A_{in}, M_{id}, and M_{in} is (are) valid for N?

- -

ANSWER:

M_{id} is valid for N since the special element 1 is in N. However, A_{in} and M_{in} are not valid for N. If n is a natural number then the additive inverse $-n$ of n is not in N. Also, the multiplicative inverse of n is not in N unless $n = 1$.

- -

We see that N satisfies all the field postulates except A_{id}, A_{in}, and M_{in}. The system N is not a field.

We return now to our discussion of mathematical induction.

There is a method of proof by mathematical induction which arises quite often in mathematics. Suppose that for each natural number n we have a mathematical proposition T_n, and that we would like to prove that T_n is true for every natural number n. Let S be the set of all the natural numbers n such that T_n is true. We would like to use the Induction Principle to prove that $S = N$. To do this we must show that

(a) 1 is in S, i.e., ____ is true, and

(b) if k is in S, then $k + 1$ is in S, i.e., ____.

- -

ANSWER:

T_1

If T_k is true, then T_{k+1} is true.

- -

This type of proof was involved in the proofs of Theorem 8.4 and 8.5. For example, in Theorem 8.4 we could let m be a fixed natural number and then, for each natural number n, let T_n be the proposition that "$m + n$ is a natural number". In the proof of Theorem 8.4 we showed first that $m + 1$ is a natural number, i.e., T_1 is true.

Then we showed that if $m + k$ is a natural number then $m + (k + 1)$ is a natural number, i.e., if T_k is true then T_{k+1} is true.

We further illustrate this type of proof with some more examples.

The reader is undoubtedly familiar with the formula for finding the sum of the first n natural numbers; $S_n = 1 + 2 + 3 + \dots + n = \frac{n(n + 1)}{2}$. Let us use the method of mathematical induction to prove this formula.

Show first that the formula is true for $n = 1$.

- -

ANSWER:

$S_1 = 1$ and $\frac{(2)(1)}{2} = 1$.

- -

Next show that if we assume the formula is true for $n = k$ then the formula will be true for $n = k + 1$. You assume that $S_k = \frac{k(k + 1)}{2}$ and try to prove that $S_{k+1} = \frac{(k + 1)(k + 2)}{2}$. Note that $S_{k+1} = S_k + (k + 1)$.

- -

ANSWER:

Assume $S_k = \frac{k(k + 1)}{2}$

$$
\begin{aligned}
\text{Then } S_{k+1} &= S_k + (k + 1) \\
&= \frac{k(k + 1)}{2} + k + 1 \\
&= (k + 1)(k/2 + 1) \\
&= (k + 1)\left(\frac{k + 2}{2}\right) \\
&= \frac{(k + 1)(k + 2)}{2}
\end{aligned}
$$

This is precisely the same value we would obtain if we substituted $k + 1$ for n in the given formula: $S_{k+1} = \frac{(k + 1)[(k + 1) + 1]}{2} = \frac{(k + 1)(k + 2)}{2}$.

We have shown that the formula $S_n = \frac{n(n + 1)}{2}$ is true when $n = 1$ and that _if_ it is true when $n = k$ _then_ it is also true when $n = k + 1$. If we let, for each natural number n, T_n be the mathematical statement that $S_n = \frac{n(n + 1)}{2}$, then we have shown that T_1 is true and that T_k implies T_{k+1}. Explain how we can conclude from the Induction Principle that T_n is true for every natural number n.

ANSWER:

Let S be the set of all natural numbers n such that T_n is true. We have shown that

(a) 1 is in S, and

(b) if k is in S, then $k + 1$ is in S.

By the Induction Principle, $S = N$. Hence T_n is true for every n.

In each proof of the preceding type there are two parts: (a) that T_1 is true, and (b) if k is a natural number such that T_k is true, then T_{k+1} is also true. Note that in part (b) we do not have to worry, _a priori_, about whether T_k is or is not true. We need only show that _if_ T_k is true _then_ T_{k+1} is also true.

The formula for the sum of the first $n + 1$ terms in a geometric progression is $G_n = a + ar + ar^2 + \ldots + ar^n = a(\frac{1 - r^{n+1}}{1 - r})$. What restriction must be put on r?

ANSWER:

$r \neq 1$, because division by zero is not allowed.

Prove the formula for the sum of the first $n + 1$ terms in a geometric progression by mathematical induction.

ANSWER:

(a) Show that $G_1 = a(\frac{1 - r^2}{1 - r})$.

$$G_1 = a + ar$$

$$a(\frac{1 - r^2}{1 - r}) = a\frac{(1 - r)(1 + r)}{1 - r} = a(1 + r) = a + ar.$$

Therefore $G_1 = a(\frac{1 - r^2}{1 - r})$.

(b) Show that if $G_k = a(\frac{1 - r^{k+1}}{1 - r})$ then $G_{k+1} = a(\frac{1 - r^{k+2}}{1 - r})$.

$$\begin{aligned} G_{k+1} &= G_k + ar^{k+1} \\ &= (a\,\frac{1 - r^{k+1}}{1 - r}) + ar^{k+1} \\ &= a\{\frac{1 - r^{k+1}}{1 - r} + r^{k+1}\} \\ &= a\{\frac{1 - r^{k+1} + (1 - r)r^{k+1}}{1 - r}\} \\ &= a\{\frac{1 - r^{k+1} + r^{k+1} - r^{k+2}}{1 - r}\} \\ &= a\{\frac{1 - r^{k+2}}{1 - r}\} \end{aligned}$$

Let S be the set of all natural numbers n such that $G_n = (a\,\frac{1 - r^{n + 1}}{1 - r})$. We have shown that 1 is in S and that if k is any natural number in S then $k + 1$ is also in S. By the Induction Principle, $S = N$. Therefore the formula is valid for every natural number n.

Prove by mathematical induction that the product of two consecutive natural numbers is an even number; i.e., $n(n + 1)$ is even for every natural number n.

ANSWER:

(a) Verify for $n = 1$.

$1(1 + 1) = 2$, which is even

(b) Show that if $k(k + 1)$ is even then

$(k + 1)([k + 1] + 1)$ is even.

$$\begin{aligned}(k + 1)([k + 1] + 1) &= (k + 1)(k + 2)\\ &= k(k + 1) + 2(k + 1)\end{aligned}$$

If $k(k + 1)$ is an even number then, since $2(k + 1)$ is an even number, their sum is even.

Let S be the set of all natural numbers n such that $n(n + 1)$ is even. We have shown that 1 is in S and that if k is any natural number in S then $k + 1$ is also in S. By the Induction Principle, $S = N$. Therefore $n(n + 1)$ is even for every natural number n.

Prove by mathematical induction that $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n(n + 1)} = \frac{n}{n + 1}$.

ANSWER:

(1) Verify for $n = 1$.

$$\frac{1}{1(1 + 1)} = \frac{1}{1 + 1}$$

(2) If $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{k(k + 1)} = \frac{k}{k + 1}$, then

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)}$$

$$= \frac{1}{k+1}(k + \frac{1}{k+2})$$

$$= \frac{1}{k+1}(\frac{k^2 + 2k + 1}{k+2})$$

$$= \frac{1}{k+1}(\frac{(k+1)^2}{k+2})$$

$$= \frac{k+1}{k+2}$$

Let S be the set of natural numbers n for which the formula is valid. We have shown that 1 is in S and that if k is any natural number in S then $k + 1$ is also in S. Therefore, by the Induction Principle $S = N$, and the formula is valid for every natural number n.

As another illustration of how the Induction Principle can be used, we will prove a theorem that will be useful in a later unit.

THEOREM 8.6: If m and q are natural numbers and $m < q$, then $q - m$ is a natural number; i.e., there is a natural number p such that $q = m + p$.

PROOF: Let S be the set of all natural numbers n such that one of the following is true:

(1) $n < m$

(2) $n = m$

(3) $n = m + p$, for some natural number p.

We will prove Theorem 8.6 by induction, showing that $S = N$. From $S = N$ we can conclude that q is in S. Why?

ANSWER:

By hypothesis in Theorem 8.6, q is a natural number; hence if $S = N$, then q is in S.

If we can prove that q is in S, then $q = m + p$, for some natural number p. Explain.

ANSWER:

By hypothesis, $q > m$. Hence, by 01 (Trichotomy), $q < m$ and $q = m$ are false. So we must have $q = m + p$, for some natural number p.

Thus we need only to prove that $S = N$.

1 is in S; i.e., $1 = m$ or $1 < m$. Why?

ANSWER:

Postulate (c) for the natural numbers.

Suppose k is in S. We must show that this implies $k + 1$ is in S for each of the three cases $k < m$, $k = m$, and $k = m + p$.

If $k < m$ then $m \neq 1$, by Postulate (c). Also $k \leq m - 1$, by Theorem 8.1 and Postulate (d). Explain why.

ANSWER:

By Theorem 8.1, if m is a natural number, $m \neq 1$, then $m - 1$ is a natural number, and by Postulate (d), there is no natural number between $m - 1$ and $(m - 1) + 1 = m$. Thus if $k < m$, then $k \leq m - 1$.

Then $k + 1 \leq m$. Thus $k + 1$ satisfies either (1) or (2) and must be in S.

Show that if $k = m$, then $k + 1$ is in S.

- -

ANSWER:

If $k = m$, then $k + 1 = m + 1$. Hence $k + 1$ is in S, since $m + 1$ has the form $m + p$, where $p = 1$.

- -

Show that if $k = m + p$, then $k + 1$ is in S.

- -

ANSWER:

If $k = m + p$, then $k + 1 = (m + p) + 1 = m + (p + 1)$. Since, by Postulate (b), $p + 1$ is a natural number if p is a natural number, then $m + (p + 1)$ has the form of (3) and $k + 1$ is in S.

- -

Hence in any case, if k is in S then $k + 1$ is also in S. By the Induction Principle, $S = N$.

Reconstruct the proof of Theorem 8.6. Do not look back over the preceding items once you have begun to write the proof.

- -

ANSWER:

THEOREM 8.6: If m and q are natural numbers and $m < q$, then $q - m$ is a natural number; i.e., there is a natural number p such that $q = m + p$.

Let S be the set of all natural numbers n such that anyone of the following is true:

(1) $n < m$

(2) $n = m$

(3) $n = m + p$, for some natural number p.

1 is in S, since either $1 < m$ or $1 = m$ by Postulate (c) for the natural numbers.

If k is in S, then $k + 1$ is in S for each of the three possible cases (1), (2), and (3).

(1) If $k < m$, then $k \leq m - 1$; hence $k + 1 \leq m$ and either (1) or (2) holds for $k + 1$.

(2) If $k = m$, then $k + 1 = m + 1$ and (3) holds for $k + 1$ with $p = 1$.

(3) If $k = m + p$, then $k + 1 = m + (p + 1)$ and (3) holds for $k + 1$.

By the Induction Principle, $S = N$. Since q is in N, q is in S. Since $q > m$, by hypothesis, $q < m$ and $q = m$ are false. Hence the only remaining possibility, $q = m + p$, for some natural p, is true. Therefore $q - m = p$ is a natural number.

ALTERNATE DEFINITION OF N

For most of us the intuitive notion that we have of the set of natural numbers is something like the following:

1 is a natural number and the other natural numbers are obtained by starting with the number 1 and successively adding ones.

This intuitive notion can be made a little more precise by stating that:

(1) 1 is a natural number, and

(2) If k is a natural number, then $k + 1$ is a natural number, and furthermore,

(3) The set of natural numbers is the "smallest" set which contains 1 and which, if it contains a number k, also contains $k + 1$.

We can rephrase this as an alternate definition of the set N of natural numbers.

DEFINITION 8.2: (Alternate Definition of N)

Let $\mathcal{I}$ be the family of all sets S of real numbers such that

(a) 1 is in S, and

(b) if x is in S, then x + 1 is in S.

(The set of *all* real numbers is a set in the family $\mathcal{I}$.) Then the set N of natural numbers is the set of those elements that are common to *every* set S in the family $\mathcal{I}$; i.e., n is in N if and only if n is in S for every set S in $\mathcal{I}$.

From the above definition of the set N, can we conclude:

(a) 1 is in N? Why?

- -

ANSWER:

Yes; by (a) 1 is in *every* set S in the family $\mathcal{I}$.

- -

Can we conclude:

(b) If x is in N, then x + 1 is in N? Why?

- -

ANSWER:

Yes. If x is in N, then x is in each set S of $\mathcal{I}$. Then, by (b), x + 1 is in each set S of $\mathcal{I}$; i.e., x + 1 is in N.

- -

We have shown that the set N satisfies both (a) and (b), so N is a set in $\mathcal{I}$. In fact it is the smallest set in $\mathcal{I}$ because it is contained in every set S in $\mathcal{I}$.

The Alternate Definition essentially amounts to the use of the Induction Principle as a definition of N. Recall that the Induction Principle states that if S is a subset of N which satisfies (a) and (b) then S is all of N; i.e., no set S smaller than N satisfies (a) and (b).

If S is a subset of N which satisfies (a) and (b) then the set S is in the collection.____ .

ANSWER:

$\mathcal{I}$

Since S is in $\mathcal{I}$, then ____ is a subset of ____.

ANSWER:

N is a subset of S.

Since S is also a subset of N, $S = N$.

We wish now to show that Postulates (c) and (d) follow from the Alternate Definition of N. Postulate (c) states that $n \geq 1$ for each number n in N. To prove Postulate (c) we will show that there is a set S in $\mathcal{I}$ which contains no number less than 1.

Prove that the set S of all real numbers x such that $x \geq 1$ is in $\mathcal{I}$.

ANSWER:

PROOF: Since $1 \geq 1$, 1 is in S. If x is in S, then $x \geq 1$. Hence $x + 1 \geq 1 + 1 > 1$. Therefore $x + 1$ is in S. It follows that S satisfies (a) and (b) and is in $\mathcal{I}$.

Since S in in $\mathcal{I}$, N is a subset of S. Hence $n \geq 1$ for each n in N.

Postulate (d): If n is in N, there is no number in N between n and $n + 1$.

We will prove Postulate (d) by induction. Let S be the set of all numbers x in N such that $x = 1$ or $x \geq 2$. Prove that S is in I.

- -

ANSWER:

PROOF: 1 is in S, by hypothesis. If x is in S then either $x = 1$ or $x \geq 2$. If $x = 1$, then $x + 1 = 2$. If $x \geq 2$, then $x + 1 \geq 3 > 2$. Hence in either case, $x + 1 \geq 2$. Since $x + 1$ is in N it must be in S. This proves that S satisfies (a) and (b), and so S is in I.

- -

Since S is in I, N is a subset of S. But S is also a subset of N. So $S = N$. This proves that there is no number in N between 1 and 2.

Assume Postulate (d) is true for $n = k$; i.e., there is no natural number between ____.

- -

ANSWER:

k and $k + 1$.

- -

We want to show this assumption implies ____.

- -

ANSWER:

there is no natural number between $k + 1$ and $(k + 1) + 1$.

- -

Let S be the subset of N consisting of all natural numbers except those natural numbers x such that $k + 1 < x < (k + 1) + 1 = k + 2$. If we can show $S = N$, then there will be no natural numbers between $k + 1$ and $(k + 1) + 1$, and the proof will be complete. We will show that S is in $\mathcal{I}$.

(a) 1 is in S. Why?

ANSWER:

(a) There is no natural number less than 1. Since k is in N, $k + 1$ is also in N. Hence $k + 1 < 1$ is impossible. Since 1 is in N, 1 is in S.

(b) Assume t is in S. Since we are assuming Postulate (d) for $n = k$, t is not between k and $k + 1$. Therefore, either $t \le k$ or $t \ge k + 1$ by O1.

We want to show from this assumption that ____ is in S.

ANSWER:

(b) $t + 1$

If $t \le k$ or $t \ge k + 1$, then $t + 1 \le$ ____ or $t + 1 \ge$ ____.

ANSWER:

$k + 1$

$k + 2$

Thus $k + 1 < t + 1 < k + 2$ is impossible. Hence $t + 1$ is in S. We have shown that S satisfies (a) and (b), and so S is in $\mathcal{I}$. It follows that N is a subset of S. But S is a subset of N.

Therefore, S = N, and the proof is complete.

Our proof of Postulate (d) using the Alternate Definition of N is based on the Induction Principle. This proof is valid because the Induction Principle is obviously true when N is defined using the Alternate Definition.

Thus we have shown that the four postulates given in our first definition of N can be proved from our second or alternate definition of N.

We can now show that the set N is uniquely defined by Definition 8.1; i.e., we can show that there is only one set of real numbers which satisfies Postulates (a) - (d) of Definition 8.1.

We have just shown that the set N defined in Definition 8.2 satisfies these four postulates. Suppose N' is a set of real numbers which satisfies Postulates (a) - (d). Which of the postulates tell us that N' is in the family *I* described in Definition 8.2?

ANSWER:
Postulates (a) and (b).

Since N' is in *I*, N is a subset of N'. But we proved the Induction Principle on the basis of Postulates (a) - (d), so it holds for N'. Now N is a subset of N' which satisfies

(a) 1 is in N, and

(b) if k is in N, then k + 1 is in N. Therefore, by the Induction Principle, N' = N.

So we conclude that the set N defined in Definition 8.2 is the only set of real numbers satisfying Postulates (a) - (d) of Definition 8.1.

PRIME NUMBERS

Write each of the following natural numbers as the product of two or more natural numbers. In some cases you will be able to do this in more than one way.

(Disregard the order of the factors.)

a. 2 = ____ • ____
b. 3 = ____ • ____
c. 4 = ____ • ____ or ____ ____
d. 5 = ____ • ____
e. 6 = ____ • ____ or ____ ____
f. 7 = ____ • ____
g. 8 = ____ • ____ or ____ ____ or ____ ____ ____
h. 9 = ____ • ____ or ____ ____
i. 10 = ____ • ____ or ____ ____
j. 11 = ____ • ____

- -

ANSWER:

a. (2 • 1)
b. (3 • 1)
c. (2 • 2 or 4 • 1)
d. (5 • 1)
e. (3 • 2 or 6 • 1)
f. (7 • 1)
g. (8 • 1 or 4 • 2 or 2 • 2 • 2)
h. (3 • 3 or 9 • 1)
i. (5 • 2 or 10 • 1)
j. (11 • 1)

- -

Which of the above numbers could be factored in only one way (without regard to the order of the factors)? ____

- -

ANSWER:

2, 3, 5, 7, 11

- -

If we continued the above process we would separate the natural numbers greater than 1 into two sets. One set would consist of those natural numbers a that can be factored as products of natural numbers in only one way, a • 1. The other set would consist of those natural numbers that can be factored as products of natural numbers in more than one way.

DEFINITION 8.3: A natural number p is said to be prime if $p > 1$ and p cannot be written as the product of two natural numbers other than p and 1. A natural number c is said to be composite if $c > 1$ and c is not prime.

Thus N may be partitioned into three sets; the set of ____, the set of ____ and the set of consisting of just the number 1.

- -

ANSWER:

primes,

composites, (either order)

- -

What are the next four primes larger than 11? ____, ____, ____, ____.

- -

ANSWER:

13, 17, 19, 23

- -

An important part of the definition of a prime number is the restriction, natural numbers, placed on the set from which we can choose our factors. Briefly, we will be factoring *over* N.

In how many ways can 7 be factored *over the real number system*?

ANSWER:

7 can be factored in an infinite number of ways over the real number system. For example, $7 = 7/2 \cdot 2 = 14/3 \cdot 3/2 = 49/211 \cdot 211/7$, etc.

The number 12 has 6 factors in N. They are ____, ____, ____, ____, ____, and ____.

ANSWER:

1, 2, 3, 4, 6, 12

THEOREM 8.7: If n is a natural number and $n = a \cdot b$, where each of a and b is a natural number different from 1, then $1 < a < n$ and $1 < b < n$.

PROOF: Since $a \neq 1$ and $b \neq 1$, $a > 1$ and $b > 1$ by Postulate ____. By Order Theorem 4.13, $1 > 0$. Hence, by O2, we have $b > 0$. Complete the proof.

ANSWER:

(c)

From $a > 1$, $b > 0$, we can conclude by O4 that $a \cdot b > 1 \cdot b$ or $n > b$. Similary, $a > 1$ and $1 > 0$ implies $a > 0$. From $b > 1$ and $a > 0$, we have $a \cdot b > a \cdot 1$ or $n > a$. Thus we have shown that $1 < a$ and $a < n$, and that $1 < b$ and $b < n$.

PRIME FACTORIZATION

THEOREM 8.8: Every n in N, $n > 1$, is either a prime or has a factorization as a product of primes which is unique except for the order of the factors.

This theorem is generally referred to by one of two names; the fundamental theorem of arithmetic or the unique factorization theorem.

We must prove that a prime factorization exists and that only one such factorization is possible.

If n is prime, there is nothing to prove. If not, then $n = a \cdot b$. If a and b are prime, we are through. If not, $a = a_1a_2$, $b = b_1b_2$, and $n = a_1a_2 \cdot b_1b_2$. If each of the factors a_i and b_i, $(i = 1, 2)$, is prime, we are through. If not, we continue as before until a prime factorization of n is obtained. This discussion provides an intuitive approach to the proof of Theorem 8.8. A precise proof using mathematical induction follows.

PROOF: (Existence) Assume that there is an n in N, $n > 1$, which is neither a prime nor a product of primes.

What theorem tells us there is a smallest such number n?

- -

ANSWER:

Theorem 8.2.

- -

Let k be the smallest such number. Let $k = ab$ where a and b are in N and $a \neq 1$, $b \neq 1$. Then $1 < a < k$ and $1 < b < k$, by Theorem 8.7.

We know that each of a and b is a prime or a product of primes. Why?

- -

ANSWER:

a and b are both less than k and k is the smallest number in N, different from 1, that is not a prime or the product of primes.

Therefore k is a product of primes. This contradicts what statement?

ANSWER:

Our original assumption that k was neither prime nor a product of primes.

Therefore our original assumption is incorrect and there is no n which is neither prime nor a product of primes. We have proved that a prime factorization of every n in N, $n > 1$, exists.

The proof that we have given is a proof by mathematical induction since it involves the Well-ordering Property Theorem 8.2.

(Uniqueness) Assume that there exists an n in N that can be factored in two different ways, where all of the factors are prime.

The Well-ordering Principle tells us there is a ____ such n.

ANSWER:

smallest, or least

Let k be the least such number n. Then $k = p_1 \cdot p_2 \cdots p_\ell = q_1 \cdot q_2 \cdots q_m$ where the p's and q's represent the prime factors in the two factorizations we have assumed. We can further assume that the factors are arranged in order of increasing size, i.e., $p_1 \leq p_2 \leq \cdots \leq p_\ell$ and $q_1 \leq q_2 \leq \cdots \leq q_m$.

Moreover, $p \neq q$ for then we could cancel the first factor in each of the decompositions and obtain two different prime factorizations of the number $u = p_2 \cdot p_3 \cdots p_\ell = q_2 \cdot q_3 \cdots q_m$. Why is this not possible?

ANSWER:

$u < k$, which would contradict our assumption that k is the smallest number in N having two different prime factorizations.

Since $p_1 \neq q_1$, by the Trichotomy Property 01 we can conclude that ____.

ANSWER:

$p_1 < q_1$ or $q_1 < p_1$.

Suppose $p_1 < q_1$. (If $q_1 < p_1$, then we would just interchange the p's and q's in the following.)

We will now form a number n' and use it to arrive at a contradiction of our original assumption that k has two factorizations.

(1) $n' = k - (p_1 \cdot q_2 \cdot q_3 \cdots q_m)$.

Substituting each of the factorizations for k in the above expression for n' we have,

$$(2) \quad \begin{aligned} n' &= (p_1 \cdot p_2 \cdots p_\ell) - (p_1 \cdot q_2 \cdots q_m) \\ &= p_1 ((p_2 \cdots p_\ell) - (q_2 \cdots q_m)) \end{aligned}$$

and

$$(3) \quad \begin{aligned} n' &= (q_1 \cdot q_2 \cdots q_m) - (p_1 \cdot q_2 \cdots q_m) \\ &= (q_1 - p_1)(q_2 \cdots q_m). \end{aligned}$$

Which of the equations tells us that $n' < k$? Why?

ANSWER:

(1) tells us that $n' < k$, because $p_1 \cdot q_2 \cdot q_3 \cdots q_m > 0$.

Which of the equations tells us that p_1 is a factor of n'?

ANSWER:

Equation (2)

Which of the equations tells that n' is a natural number? Why?
(Hint: Remember $p_1 < q_1$)

ANSWER:

Equation (3). Since $p_1 < q_1$, $(q_1 - p_1)$ will be a natural number by Theorem 8.6, therefore n' is a natural number because the set of natural numbers is closed under multiplication.

The facts that n' is in N and that $n' < k$ allow us to make what statement about the factorization of n'? [Note that $n' \neq 1$ because p_1 is a factor of n'.]

ANSWER:

The factorization of n' is unique because k is the smallest number in N having two different prime factorizations.

Then p_1 must be a factor in this unique factorization of n'. Why?

ANSWER:

p_1 is prime, and p_1 is a factor of n' from equation (2).

- -

Recall from equation (3) that

$n' = (q_1 - p_1) \cdot (q_2 \cdot q_3 \ldots q_m)$.

Since $(q_1 - p_1)$ is a natural number, then both $(q_1 - p_1)$ and $(q_2 \cdot q_3 \ldots q_m)$ can be written as a product of prime factors. We wish to show that p_1 is not a factor of this decomposition of $(q_1 - p_1)$ and $(q_2 \cdot q_3 \ldots q_m)$, thus arriving at a contradiction.

Can p_1 be a factor of $(q_2 \cdot q_3 \ldots q_m)$? Why?

(Hint: Recall that $p_1 < q_1 \leq q_2 \leq q_3 \ldots \leq q_m$.)

- -

ANSWER:

No; p_1 and all the q's are prime. If p_1 were a factor of $(q_2 \cdot q_3 \ldots q_m)$, it would have to equal one of the q's, but p_1 is less than each of them. (Remember that the prime factorization $q_2 \cdot q_3 \ldots q_m$ is unique because $q_2 \cdot q_3 \ldots q_m < k$.)

- -

Show that p_1 is not a factor of $(q_1 - p_1)$. Why? (Hint: Assume that p_1 is a factor of $(q_1 - p_1)$, then $q_1 - p_1 = h \cdot p_1$, where h is some natural number.)

- -

ANSWER:

If p_1 is a factor of $q_1 - p_1$, then $q_1 - p_1 = h \cdot p_1$, where h is some natural number. $q_1 - p_1 = h \cdot p_1$ implies that $q_1 = p_1h + p_1 = p_1(h + 1)$.

But $q_1 \neq p_1(h + 1)$ because q_1 is prime.

- -

We have arrived at a contradiction. What is it?

ANSWER:

p_1 is a factor of n' and p_1 is not a factor of n'.

Since we have arrived at a contradiction, our original assumption that k has two prime factorizations is false; and we have proved that the prime factorization of any n in N is unique.

Review the preceding items and then reconstruct the proof of the uniqueness part of Theorem 8.8. Do not look back, once you have begun to write the proof.

ANSWER:

THEOREM 8.8: Every n in N, $n > 1$, is either a prime or has a factorization as a product of primes which is unique except for the order of the factors.

PROOF: (Uniqueness) Assume that there exists an n in N that can be factored in two different ways, where all of the factors are prime. The Well-ordering Principle, Theorem 8.2, tells us there is a smallest such n. Call it k.

Then $k = p_1 \cdot p_2 \cdots p_\ell = q_1 \cdot q_2 \cdots q_m$ where the p's and q's represent the prime factors in the two factorizations we have assumed. We further assume that the factors are arranged in order of increasing size, i.e., $p_1 \leq p_2 \leq \cdots \leq p_\ell$ and $q_1 \leq q_2 \leq q_3 \cdots \leq q_m$.

Moreover, $p_1 \neq q_1$. For if $p_1 = q_1$ we could cancel the first factor in each of the decompositions and obtain two different prime factorizations of the number $u = p_2 \cdot p_3 \cdots p_\ell = q_2 \cdot q_3 \cdots q_m$. Since $u < k$, this contradicts our assumption that k is the smallest number in N with two prime factorizations.

Since $p_1 \neq q_1$, by O1 (Trichotomy) we have $p_1 < q_1$ or $q_1 < p_1$. We assume $p_1 < q_1$, and arrive at a contradiction. (If $q_1 < p_1$, then we would interchange the p's and q's in the following and arrive at the same contradiction). Since, by assumption, $p_1 < q_1$, we have $p_1 \cdot q_2 \cdot q_3 \cdots q_m < q_1 \cdot q_2 \cdot q_3 \cdots q_m = k$; and by Theorem 8.7, $k = p_1 \cdot q_2 \cdot q_3 \cdots q_m$ is a natural number. Let

$$(1) \quad n' = k - p_1 \cdot q_2 \cdot q_3 \cdots q_m.$$

Substituting each of the prime factorizations for k in the above expression for n', we have

$$\begin{aligned}(2) \quad n' &= (p_1 \cdot p_2 \cdots p_\ell) - (p_1 \cdot q_2 \cdots q_m)\\ &= p_1((p_2 \cdots p_\ell) - (q_2 \cdots q_m))\end{aligned}$$

and

$$\begin{aligned}(3) \quad n' &= (q_1 \cdot q_2 \cdots q_m) - (p_1 \cdot q_2 \cdots q_m)\\ &= (q_1 - p_1)(q_2 \cdots q_m).\end{aligned}$$

We know n' is in N, and from (1), $n' < k$. Hence the factorization of n' is unique since k is the smallest number in N having two prime factorizations.

From equation (2) we know p_1 is a factor in this unique factorization of n'. We will now use equation (3) to show that p_1 is not a factor in this unique factorization of n', hence arriving at a contradiction.

In (3), p_1 is not a factor of $(q_2 \cdots q_m)$ because p_1 and all the q's are prime and $p_1 < q_1 \leq q_2 \cdots \leq q_m$. ($q_2 \cdot q_3 \cdots q_m < n'$, so the factorization of $q_2 \cdot q_3 \cdots q_m$ is unique.) If p_1 is a factor of $(q_1 - p_1)$, then $q_1 - p_1 = h \cdot p_1$ where h is some natural number, which implies $q_1 = p_1(h + 1)$. But $q_1 \neq p_1(h + 1)$ because q_1 is prime; hence p_1 is not a factor of $(q_1 - p_1)$.

Thus we have arrived at the contradiction that p_1 is a factor of n' and p_1 is not a factor of n'. Hence our original assumption that k has two different prime factorizations is false and we have proved that the prime factorization of any n in N is unique.

An interesting corollary to this theorem is:

Corollary: If a prime p is a factor of ab, then p must be a factor of either a or b.

Prove the corollary using Theorem 8.8.

ANSWER:

If p is a factor of the natural number ab then ab = ps, s in N. The product of p times the prime decomposition of s would yield a prime decomposition of ab containing p.

If p is not a factor of either a or b then the product of the prime decompositions of a and b would yield a prime decomposition of ab not containing p as a factor. This would contradict the fact that the prime factorization of ab is unique.

The following examples illustrate an algorithm that gives a systematic method for finding the prime factorization of a number.

Find the prime factorization of 308.

Divide 308 and the successive quotients by the prime numbers in order of increasing magnitude.

successive quotients	308	2	(Divide by 2 since 308 is even)
	154	2	(Divide by 2 again since 154 is even)
	77	7	(Divide by 7; 77 is not divisible by 2, 3, or 5)
	11	11	(Final quotient is a prime number)

Therefore $308 = 2^2 \cdot 7 \cdot 11$.

THEOREM 8.9: Let n be a natural number, $n > 1$. If n is not a prime then n has a prime divisor p such that $p^2 \leq n$.

PROOF: Suppose n is not a prime. Then $n = a \cdot b$, where a and b are natural numbers and $1 < a < n$, $1 < b < n$. Each of a and b has a prime factor, by ____.

- -

ANSWER:

Theorem 8.8.

- -

Suppose p is a prime factor of a and q is a prime factor of b. Show that it is impossible that both $p^2 > n$ and $q^2 > n$.

- -

ANSWER:

Assume $p^2 > n$ and $q^2 > n$. pq is a factor of ab, so $pq \leq ab = n$. Suppose $p \geq q$. Then $pq \geq q^2 > n$, a contradiction. If $p \leq q$ then $pq \geq p^2 > n$, also a contradiction.

Therefore either p or q is a prime factor of n with square less than or equal to n. This proves the theorem.

- -

Find the prime factorization of 211.

Since 2, 3, 5, 7, 11, 13 are not divisors of 211 we know that 211 is a prime without trying any prime number greater than 13. Why?

- -

ANSWER:

By Theorem 8.9 it is not necessary to use any primes greater than $\sqrt{n}$ as trial divisors when finding the prime factorization of a natural number n.

- -

Find the prime factorization of 210.

- -

ANSWER:

$210 = 2 \cdot 3 \cdot 5 \cdot 7$

- -

Find the prime factorization of 44982.

- -

ANSWER:

$44982 = 2 \cdot 3^3 \cdot 7^2 \cdot 17$

- -

DEFINITION 8.4: The least common multiple, l.c.m., of a pair of natural numbers is the smallest natural number which has each of the numbers as a divisor (factor).

The prime factorization of a natural number is valuable in finding the l.c.m. of two or more natural numbers.

Example: Find the l.c.m. of 60 and 90.

$60 = 2^2 \cdot 3 \cdot 5$ and $90 = 2 \cdot 3^2 \cdot 5$.

Since 60 and 90 are factors of their l.c.m., the l.c.m. must contain the factors of each number. Therefore the l.c.m. of 60 and 90 is $2^2 \cdot 3^3 \cdot 5 = 180$.

Find the least common multiple of 57 and 95.

- -

ANSWER:

$57 = 3 \cdot 19$

$95 = 5 \cdot 19$

l.c.m. of 57 and 95 is $3 \cdot 5 \cdot 19 = 285$.

- -

Find the least common multiple of 432 and 648.

ANSWER:

$432 = 2^4 \cdot 3^3$

$648 = 2^3 \cdot 3^4$

l.c.m. of 432 and 648 is $2^4 \cdot 3^4 = 1296$.

This process of finding the least common multiple gives us a systematic way of finding the lowest common denominator when adding or subtracting fractions.

Example: Find the sum: 1/75 + 2/45.

$$\begin{aligned} 1/75 + 2/45 &= \frac{1}{3 \cdot 5 \cdot 5} + \frac{2}{3 \cdot 3 \cdot 5} \\ &= \frac{1}{3 \cdot 5 \cdot 5} \cdot \frac{3}{3} + \frac{2}{3 \cdot 3 \cdot 5} \cdot \frac{5}{5} \\ &= \frac{3}{3 \cdot 3 \cdot 5 \cdot 5} + \frac{10}{3 \cdot 3 \cdot 5 \cdot 5} \\ &= \frac{13}{3 \cdot 3 \cdot 5 \cdot 5} \\ &= \frac{13}{225} \end{aligned}$$

Notice that leaving the denominators in factored form tells us that the final fraction cannot be reduced since the primes 3, 5, are not factors of 13.

Find the following sums. (Show your work.)

(a) 3/14 - 4/35

ANSWER:

(a) $$\begin{aligned} 3/14 - 4/35 &= \frac{3}{2 \cdot 7} - \frac{4}{5 \cdot 7} \\ &= \frac{15}{2 \cdot 5 \cdot 7} - \frac{8}{2 \cdot 5 \cdot 7} \\ &= \frac{7}{2 \cdot 5 \cdot 7} \\ &= \frac{1}{10} \end{aligned}$$

(b) $\frac{3}{5} + \frac{7}{75} - \frac{5}{63}$

ANSWER:

(b) $$\begin{aligned} \frac{3}{5} + \frac{7}{75} - \frac{5}{63} &= \frac{3}{5} + \frac{7}{3 \cdot 5 \cdot 5} - \frac{5}{3 \cdot 3 \cdot 7} \\ &= \frac{3 \cdot 3 \cdot 3 \cdot 5 \cdot 7}{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7} + \frac{7 \cdot 3 \cdot 7}{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7} - \\ &\quad \frac{5 \cdot 5 \cdot 5}{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7} \\ &= \frac{945 + 147 - 125}{3^2 \cdot 5^2 \cdot 7} \\ &= \frac{967}{3^2 \cdot 5^2 \cdot 7} \\ &= \frac{967}{1575} \end{aligned}$$

DEFINITION 8.5: The greatest natural number that divides each of a pair of natural numbers is called the greatest common divisor, g.c.d., of the pair.

The prime factorization of a natural number also allows us to treat systematically the problem of finding the greatest common divisor (g.c.d.). Let us use 60 and 90 once again to illustrate how to find the greatest common divisor.

We first write down the prime factorizations of 60 and 90.

$60 = 2 \cdot 2 \cdot 3 \cdot 5$

$90 = 2 \cdot 3 \cdot 3 \cdot 5$

From these factorizations we see immediately that the greatest common divisor of 60 and 90 is $2 \cdot 3 \cdot 5 = 30$.

What is the greatest common divisor of 21 and 91?

- -

ANSWER:

$21 = 3 \cdot 7$

$91 = 7 \cdot 13$

$\therefore$ g.c.d. = 7.

- -

What is the g.c.d. of 432 and 648?

- -

ANSWER:

$432 = 2^4 \cdot 3^3$

$648 = 2^3 \cdot 3^4$

$\therefore$ g.c.d. $= 2^3 \cdot 3^3 = 216$.

- -

This method of finding the greatest common divisor allows us to treat the reduction of fractions systematically.

Example: $\frac{24}{36} = \frac{2^3 \cdot 3}{2^2 \cdot 3^2} = \frac{2}{3} \cdot \frac{2^2 \cdot 3}{2^2 \cdot 3} = \frac{2}{3}$, since $\frac{2^2 \cdot 3}{2^2 \cdot 3} = 1$

$2^2 \cdot 3$ is the ____ of 24 and 36.

- -

ANSWER:

greatest common divisor

Write the following fraction in reduced form. (Show your work).

$$\frac{385}{455}$$

ANSWER:

$$\frac{385}{455} = \frac{5 \cdot 7 \cdot 11}{5 \cdot 7 \cdot 13} = \frac{5 \cdot 7}{5 \cdot 7} \cdot \frac{11}{13} = \frac{11}{13}$$

COUNTABILITY

DEFINITION 8.6: We say that a non-empty set B is *countable* if there is a reversible function F whose domain is the set of natural numbers and whose range is the set B.

Recall that if F is a function from X *to* Y, the domain of F is ____, and the range of F is ____.

ANSWER:

X,

a subset of Y.

If the range of F *is* all of Y, we say F is a function from X ____ Y.

ANSWER:

onto

Thus every function is a function from its ____ onto its ____.

ANSWER:

domain

range.

Recall, too, that if F is a reversible function then F sets up a correspondence between the elements of its domain and the elements of its range such that each element of the domain corresponds to ____ and each element of the range corresponds to ____.

ANSWER:

exactly one element of the range,

exactly one element of the domain.

If F is a reversible function from X onto Y, we say that F defines a one-to-one correspondence between the elements of X and the elements of Y. Thus we say a set is countable if its elements can be put into a one-to-one correspondence with the elements of N.

If f is a function from X onto Y and if x is the element in the domain that is mapped onto y by the function f, we sometimes denote this by writing $x \xrightarrow{f} y$. Using the above notation, show a function f from N onto the set of even natural numbers.

ANSWER:

$1 \xrightarrow{f} 2$
$2 \xrightarrow{f} 4$
$3 \xrightarrow{f} 6$
$4 \xrightarrow{f} 8$
$\cdot \qquad \cdot$
$\cdot \qquad \cdot$
$\cdot \qquad \cdot$
$n \xrightarrow{f} 2n$
$\cdot \qquad \cdot$
$\cdot \qquad \cdot$
$\cdot \qquad \cdot$

or, f is a function such that if n is a natural number, then $n \xrightarrow{f} 2n$.

The above example shows that the set of even natural numbers is ____.

ANSWER:

countable.

THE ARCHIMEDEAN PROPERTY

The Completeness Property of the real number system allows us to prove the following theorem.

THEOREM 8.10: The set N of natural numbers has no upper bound.

PROOF: If N has an upper bound then the Completeness Property tells us that ____.

ANSWER:

N has a least upper bound.

Assume that N has an upper bound and let u denote the l.u.b. of N. Then $u - 1$ is not an upper bound of N. So there is a natural number n such that $u - 1 < n$. Then $u < n + 1$. Why does this give us a contradiction?

ANSWER:

Since n is a natural number, $n + 1$ is also in N. But $u < n + 1$ contradicts the assumption that u is an upper bound of N.

An immediate consequence of Theorem 8.10 is the following theorem which is called the Archimedean Property.

THEOREM 8.11: If a and b are positive real numbers, there is a natural number n such that $na > b$.

PROOF: There is a natural number n such that $n > b/a$. Why?

ANSWER:

By Theorem 8.10, b/a is not an upper bound of N.

From $n > b/a$ we get $na > b$, which proves the theorem.

Taking $b = 1$ in Theorem 8.11 we obtain

THEOREM 8.12: If a is a positive real number, there is a natural number n such that $1/n < a$.

PROOF: By Theorem 8.11 there is a natural number n such that $n \cdot a > 1$. Then $a > 1/n$.

Let S be the set of all numbers of the form $1/n$ such that n is a natural number. The preceding result tells us that ____ is the greatest lower bound of S.

ANSWER:

zero.

REVIEW ITEMS

1. What field postulates fail to hold for N?

ANSWER:

A_{id}, A_{in}, M_{in}.

---

2. Find the prime factorization of 99,999.

ANSWER:

$3 \cdot 3 \cdot 41 \cdot 271$

---

3. Which of the following sets of numbers are well-ordered?

(a) The odd integers.

(b) The positive even integers.

(c) The non-negative real numbers.

(d) The set of numbers of the form 2^k where k is a natural number.

ANSWER:

(b) and (d). ((a) fails because the set has no least element. The set (c) has a least element, viz. 0, but the subset of real numbers between 0 and 1 has no least element.)

---

4. Prove the following statement is correct by mathematical induction:

$n^3 - n$ is divisible by 3 for all natural numbers n.

- -

ANSWER:

Let S be the set of all natural numbers n for which the statement is correct.

(a) 1 is in S because $1^3 - 1 = 0$ is divisible by 3.

(b) Assume k is in S; i.e., $k^3 - k$ is divisible by 3 for some natural number k. Then

$$\begin{aligned}(k + 1)^3 - (k + 1) &= k^3 + 3k^2 + 3k + 1 - (k + 1)\\ &= (k^3 - k) + (3k^2 + 3k)\end{aligned}$$

and this last expression is divisible by 3 if $k^3 - k$ is divisible by 3. Therefore, $k + 1$ is in S if k is in S.

Therefore $S = N$, by the Induction Principle. So the statement is correct for every natural number n.

- -

5. Find the l.c.m. of 35 and 75.

- -

ANSWER:

$5^2 \cdot 3 \cdot 7$ or 525

- -

6. Find the g.c.d. of 231 and 546.

- -

ANSWER:

$3 \cdot 7$ or 21

- -

7. Which of the following subsets of N is (are) closed under addition?

(a) The odd natural numbers.

(b) The even natural numbers.

(c) Numbers of the form 2^k where k is a natural number.

ANSWER:

(b)

8. Which of the above sets are closed under multiplication?

ANSWER:

(a), (b), (c).

9. Prove that the formula $3 + 3^2 + 3^3 + \ldots + 3^n = \dfrac{3^{n+1} - 3}{2}$ is correct for all natural numbers n by mathematical induction.

ANSWER:

Let S be the set of all natural numbers for which the formula is correct.

(a) If $n = 1$, we have $\dfrac{3^{1+1} - 3}{2} = \dfrac{3^2 - 3}{2} = \dfrac{6}{2} = 3$, hence the formula is correct for $n = 1$, and 1 is in S.

(b) If $n = k$, we have

(1) $3 + 3^2 + 3^3 + \ldots + 3^k = \dfrac{3^{k+1} - 3}{2}$

If $n = k + 1$, we have

(2) $3 + 3^2 + 3^3 + \ldots + 3^k + 3^{k+1} = \dfrac{3^{(k+1)+1} - 3}{2} = \dfrac{3^{k+2} - 3}{2}$

We want to show that (1) implies (2).

Addding 3^{k+1} to both sides of (1) we obtain

$$(3)\quad 3 + 3^2 + 3^3 + \dots + 3^k + 3^{k+1} = \frac{3^{k+1} - 3}{2} + 3^{k+1} \quad \Longrightarrow$$

$$(4)\quad = \frac{3^{k+1} - 3 + 2 \cdot 3^{k+1}}{2} \quad \Longrightarrow$$

$$(5)\quad = \frac{3 \cdot 3^{k+1} - 3}{2} \quad \Longrightarrow$$

$$(6)\quad = \frac{3^{k+2} - 3}{2}$$

Equation (6) is identical to equation (2) and since (1) $\Longrightarrow$ (6), then (1) $\Longrightarrow$ (2), and $k + 1$ is in S if k is in S. Therefore $S = N$. So the formula is correct for every natural number n.

- -

10. Show that the set of squares of the natural numbers is countable; i.e., define a function f that maps the set of natural numbers onto to the set of squares of the natural numbers.

- -

ANSWER:

$$\begin{array}{ccc} 1 & \xrightarrow{f} & 1 \\ 2 & \xrightarrow{f} & 4 \\ 3 & \xrightarrow{f} & 9 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ n & \xrightarrow{f} & n^2 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \end{array}$$

or, f is a function such that if n is a natural number, then $n \xrightarrow{f} n^2$

- -

IX. INTEGERS

DEFINITION OF THE SET OF INTEGERS

As was the case with the natural numbers, in this unit we will consider the integers as a subsystem of the real numbers. We will develop some of the properties that are peculiar to the integers and introduce some terms and concepts that will be useful in a later unit on polynomials. We will denote the set of integers by I.

DEFINITION 9.1: The set of integers, I, consists of the set of natural numbers, the additive inverses of the natural numbers, and the number 0.

From the above definition, Definition 4.1, and Definition 8.1, it follows that the set N of natural numbers is the set of positive integers. Also, by Definition 4.1 and Order Theorem 4.5, the set of additive inverses of the natural numbers is the set of negative integers.

The integer ____ is neither positive nor negative.

- -

ANSWER:

zero

- -

In high school algebra many of the properties of integers are often taken for granted. In fact the integers are usually not defined sufficiently precisely in most traditional texts to permit meaningful proofs of the properties to be given. An example is the property that addition and multiplication of integers are closed operations. We have at times in this course tacitly assumed this and certain other properties of the integers. In this unit we will show how many of these properties can be deduced on the basis of Definition 9.1 and the postulates which have been previously assumed.

Since the integers have been defined in terms of the natural numbers, we can prove closure of addition and multiplication of integers by using the closure properties of these operations in N (Theorems 8.4 and 8.5). To prove closure of addition of integers, we note first that if a is any integer then a + 0 is an integer by Postulate ____.

- -

ANSWER:

A_{id}.

- -

If a and b are non-zero integers then there are three cases: (1) a and b are natural numbers, (2) a and b are additive inverses of natural numbers, (3) of a and b, one is a natural number and the other is the additive inverse of a natural number.

Case (1). a and b are natural numbers. In this case a + b is a natural number, and therefore an integer, by ____.

- -

ANSWER:

Theorem 8.4.

- -

Case (2). $a = -k$, $b = -\ell$, where k and ℓ are natural numbers.

Show that a + b is an integer in this case. You need not list reasons.

- -

ANSWER:

$a + b = -k + -\ell = -(k + \ell)$. $k + \ell$ is a natural number; so $a + b$ is the additive inverse of a natural number, and is therefore an integer.

Case (3). a is a natural number and $b = -\ell$ where ℓ is a natural number. Prove that $a + b$ is an integer. Consider the possibilities $a > \ell$, $a = \ell$, $a < \ell$. Reasons are not required.

ANSWER:

If $a > \ell$, then $a - \ell$ is a natural number; so $a + b = a - \ell$ is an integer.

If $a = \ell$, then $a - \ell = 0$; so $a + b = a - \ell$ is an integer.

If $a < \ell$, then $\ell - a$ is a natural number; so $a + b = a - \ell = -(\ell - a)$ is the additive inverse of a natural number, and thus is an integer.

Show that if a and b are integers then $a \cdot b$ is an integer. Reasons are not required. [First show that if a or b is zero, then $a \cdot b$ is an integer. For $a \neq 0$ and $b \neq 0$, consider three cases.]

ANSWER:

First note that if a is any integer, then $a \cdot 0 = 0$. Hence $a \cdot 0$ is an integer.

Then there are three cases.

Case (1): a and b are natural numbers. In this case $a \cdot b$ is a natural number; so $a \cdot b$ is an integer.

Case (2): $a = -k$, $b = -\ell$, where k and ℓ are natural numbers. In this case $k \cdot \ell$ is a natural number. Then $a \cdot b = (-k) \cdot (-\ell) = k \cdot \ell$, so $a \cdot b$ is a natural number and thus is an integer.

Case (3): a is a natural number and $b = -\ell$ where ℓ is a natural number. In this case $a \cdot \ell$ is a natural number. So $a \cdot b = a \cdot (-\ell) = -(a \cdot \ell)$ is the additive inverse of a natural number, and hence is an integer.

Is subtraction of integers a closed operation? Why or why not?

ANSWER:

Yes. If a and b are integers, then $b - a = b + (-a)$. Since $-a$ is also an integer, the closure of addition of integers tells us that $b - a$ is an integer.

Addition and multiplication are closed operations in the set N of natural numbers and also in the set I of integers. For each of the field postulates listed in Unit II we can ask whether the postulate is valid in N or in I. If you look carefully at the set of field postulates you will see that they can be grouped into two subsets, the set $\{A_a, A_c, M_a, M_c, D\}$ and the set $\{A_{id}, A_{in}, M_{id}, M_{in}\}$. There is an important difference between the postulates in the first set and those in the second set. Each of A_a, A_c, M_a, M_c, and D gives an equation which must be satisfied by arbitrary real numbers. Because of the nature of these postulates they are automatically valid for any subset of R which is closed under addition and multiplication. In particular they are valid for N and I. For example, if a, b, c are natural numbers, then a, b, c are real numbers; hence $(a + b) + c = a + (b + c)$ by A_a for real numbers.

On the other hand the postulates A_{id}, A_{in}, M_{id}, and M_{in} are existence type postulates; i.e., they state the existence of special real numbers. For example, A_{id} states the existence of an additive identity element in the set of real numbers. The existence postulates are not necessarily valid in a subset of R because the special real number which is stated to exist need not be in the subset. For example, we know that 0 is not an element of N, so the Postulate ____ is not valid for N.

- -

ANSWER:

A_{id}

- -

Of the postulates A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, M_{in}, D,

(a) which are valid for N? List them.

(b) which are valid for I? List them.

- -

ANSWER:

(a) A_a, A_c, M_a, M_c, M_{id}, D

(b) A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, D

- -

Is N a field? ____

Is I a field? ____

- -

ANSWER:

No; A_{id}, A_{in}, and M_{in} are not valid.

No; M_{in} is not valid.

- -

Is subtraction a closed operation in N? ____, in I? ____

- -

ANSWER:

No

Yes

- -

DEFINITION 9.2: In each of the systems N and I, elements that have inverses under multiplication in the system are called units.

The system N has only one unit; what is it?

- -

ANSWER:

The number one.

- -

Two elements of I are units. What are they?

- -

ANSWER:

1, -1

- -

If a and b are integers, $b \neq 0$, then we say that a is a multiple of b and that b is a divisor or factor of a if there is an integer q such that $a = q \cdot b$.

If a and b are positive integers and b is a divisor of a, then $b \leq a$. To see this, suppose that $a = q \cdot b$, where q is an integer.

If $q = 0$, then $a = q \cdot b$ ____ 0. (Insert <, =, or >.)

If $q < 0$, then $a = q \cdot b$ ____ 0.

Since by hypothesis a ___ 0, we must have q ___ 0. Then q ___ 1, which implies that $q \cdot b$ ___ $1 \cdot b$, i.e., $a \geq b$.

- -

ANSWER:

$q \cdot b = 0$

$q \cdot b < 0$

$a > 0, \quad q > 0$

$q \geq 1, \quad q \cdot b \geq 1 \cdot b$

- -

DIVISION WITH REMAINDER

Although we do not always obtain an integer when we divide an integer by a non-zero integer, we do carry out division with remainder in I, based on the following theorem:

THEOREM 9.1: If a and b are in I, $b \neq 0$, then there exist q and r in I such that $a = bq + r$ and $0 \leq r < |b|$. (q is the quotient and r is the remainder.)

PROOF:

If a is a multiple of b, then $a = bq + r$ where q is an integer, and r is ____. Therefore the theorem is true when a is a multiple of b.

- -

ANSWER:

zero.

- -

The proof of Theorem 9.1 when a is not a multiple of b is in two parts:

Case 1: Assume $b > 0$. Since a is not a multiple of b it will lie between two consecutive multiples of b, $bq < a < b(q + 1) = bq + b$. From the first inequality, $0 < a - bq$, and from the second inequality $a - bq < b$. Letting $r = a - bq$, we have $a = bq + r$ and $0 < r < b = |b|$. Therefore the theorem is true.

Case 2: Assume that $b < 0$. Complete the proof for this case. (Hint: Use Order Theorem 4.6.)

- -

ANSWER:

Assume $b < 0$. Then $-b > 0$ by Order Theorem 4.6. From the proof of Case 1, we have $a = -b \cdot q + r = b \cdot (-q) + r$ and $0 < r < -b = |b|$. Therefore, the theorem is true. (The integer $-q$ here takes the place of q in the theorem.)

- -

Note: In Case 1, a proof that a lies between two consecutive multiples of b can be given based on mathematical induction. We will not belabor this point here.

Let us illustrate the theorem by means of an example. We divide 1763 by 95 and state the results in the form $a = bq + r,\ 0 \leq r < |b|$.

$$\begin{array}{r} 18 \\ 95\overline{)1763} \\ \underline{95} \\ 813 \\ \underline{760} \\ 53 \end{array}$$

$\therefore 1763 = 95(18) + 53$ (Here, $a = 1763$, $b = 95$, $q = 18$, $r = 53$.)

Perform the following divisions and state the results in the form $a = bq + r$.

a) Divide 547 by (-19).

- -

ANSWER:

$547 = (-19)(-28) + 15.$

- -

b) Divide -363 by 17.

- -

ANSWER:

$-363 = 17(-22) + 11$. Remember: r must be non-negative.

---

c) Divide -146 by -13.

ANSWER:

$-146 = (-13)(12) + 10$.

DECIMAL REPRESENTATION AND USE OF OTHER BASES

You may be acquainted with other methods of expressing numbers than the familiar decimal system, i.e., methods that use a base different from 10, such as base 5, base 2, etc. For example, the number 423 in base ten means $3 + 2 \cdot 10^1 + 4 \cdot 10^2$. In base 5, 423 means $3 + 2 \cdot 5^1 + 4 \cdot 5^2$, or 113 in base ten.

In base 8, 423 means ____ or ____ in base ten.

ANSWER:

$3 + 2 \cdot 8^1 + 4 \cdot 8^2$

275

It should be clear that the use of base 10, 5, 2, etc. is just a notational scheme for writing numbers.

THEOREM 9.2: If b is any integer greater than 1, then any positive integer d may be represented in base b as follows:

(A) $d = c_0 + c_1b + c_2b^2 + \ldots + c_nb^n$, where $c_0, c_1, c_2, \ldots, c_n$ are integers greater than or equal to zero and less than b.

We will agree to call this representation, (A), the expanded numeral representation of the integer d to base b.

A rigorous proof of Theorem 9.2 can be given by induction using Theorem 9.1. Instead of giving this proof we will indicate a method for obtaining the form (A) for a number, using Theorem 9.1.

In Theorem 9.2, from what set is n chosen?

- -

ANSWER:

The set of non-negative integers.

- -

From what set are $c_0, c_1, c_2, \ldots, c_n$ chosen?

- -

ANSWER:

The set of non-negative integers less than b, i.e., $\{0, 1, 2, \ldots, b - 1\}$.

- -

What are the possible values for the numbers $c_0, c_1, \ldots, c_n$ in base 10? ____; base 7? ____; base 2? ____.

- -

ANSWER:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9;
0, 1, 2, 3, 4, 5, 6;
0, 1.

- -

We will show how to derive formula (A) above by applying Theorem 9.1 to a given positive integer d and base b as follows:

(1) $d = d_1 b + c_0, \quad 0 \le c_0 < b.$

If $d_1 \le b - 1$, we are finished, taking $c_1 = d_1$. If, however, $d_1 > b - 1$, we apply the theorem again, obtaining

(2) $d_1 = d_2b + c_1, \quad 0 \leq c_1 < b.$

Substituting this expression in (1), we obtain

(3) $d = (d_2b + c_1)b + c_0 = d_2b^2 + c_1b + c_0.$

Again, if $d_2 \leq b - 1$, we are finished, taking $c_2 = d_2$. But if $d_2 > b - 1$, we apply the theorem, obtaining: ____

- -

ANSWER:

(4) $d_2 = d_3b + c_2, \quad 0 \leq c_2 < b.$

- -

Substitute equation (4) into equation (3), and show the result.

- -

ANSWER:

(5) $d = d_3b^3 + c_2b^2 + c_1b + c_0.$

- -

We continue this process until a quotient, d_n, less than b is obtained; i.e., $d_{n-1} =$ ____.

- -

ANSWER:

$d_nb + c_{n-1}, \quad 0 \leq c_{n-1} < b.$

- -

Since $d_n < b$ we may take $d_n = c_n$.

Using the above notation, write the complete equation for d if $d_4 \leq b - 1$.

- -

ANSWER:

$d = d_4b^4 + c_3b^3 + c_2b^2 + c_1b + c_0$. This is obtained as follows:

$$\begin{aligned} d = d_1b + c_0 = (d_2b + c_1)b + c_0 &= [(d_3b + c_2)b + c_1]b + c_0 \\ &= \{[(d_4b + c_3)b + c_2]b + c_1\}b + c_0 \\ &= \{[d_4b^2 + c_3b + c_2]b + c_1\}b + c_0 \\ &= (d_4b^3 + c_3b^2 + c_2b + c_1)b + c_0 \\ &= d_4b^4 + c_3b^3 + c_2b^2 + c_1b + c_0 \end{aligned}$$

Compare the equation in the answer above to the equation

(A) $d = c_0 + c_1b + c_2b^2 + \ldots + c_nb^n$.

Do the equations have the same form?

ANSWER:

Yes (Since $d_4 \leq b - 1$, we can take $c_4 = d_4$.)

Example: Express the number 95 (base ten) in base seven -- first as an expanded numeral, then as a numeral.

Solution: Using Theorem 9.1 we obtain the form (A) as follows:

$95 = 13 \cdot 7 + 4$ where $d_1 = 13$ and $c_0 = 4$

$13 = 1 \cdot 7 + 6$ where $d_2 = 1$ and $c_1 = 6$

Then

$95 = (1 \cdot 7 + 6) \cdot 7 + 4 = 1 \cdot 7^2 + 6 \cdot 7 + 4.$

Therefore, $95 = 4 + 6 \cdot 7 + 1 \cdot 7^2$ as an expanded numeral, and, by taking the remainders 4, 6, 1, in reverse order, we obtain the numeral 164 (base seven) for the number 95 (base ten).

Find the expanded numeral representation of 95 (base ten) in base 2.

Also, represent 95 (base ten) as a numeral in base two. Show your work.

- -

ANSWER:

$95 = 47 \cdot 2 + 1$

$47 = 23 \cdot 2 + 1$

$23 = 11 \cdot 2 + 1$

$11 = 5 \cdot 2 + 1$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$1 = 0 \cdot 2 + 1$

$\therefore 95 = 1 + 1 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6$ as an expanded numeral, and 95 (base ten) = 1011111 (base 2).

- -

Represent 113 (base ten) as an expanded numeral in base three and as a numeral in base three.

- -

ANSWER:

$113 = 2 + 1 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4$

and 113 (base ten) = 11012 (base three).

- -

EUCLID'S ALGORITHM

Theorem 9.1 gives us another method for solving a problem we discussed in the section on natural numbers; i.e., finding the greatest common divisor of two numbers. Recall the notation g.c.d. (a, b) for the greatest common divisor of a and b.

DEFINITION 9.3: If a and b are integers, not both zero, then the g.c.d. (a, b) is the greatest positive integer that divides a and b.

Thus, for example, g.c.d. $(15, -10) = 5$.

Our new method of finding the g.c.d. of two numbers is based on the following theorem.

THEOREM 9.3: If $a = bq + r$, $b \neq 0$, then g.c.d. $(a, b) =$ g.c.d. (b, r).

In our proof of Theorem 9.3 we will first show that if an integer divides both a and b, it also divides r; and conversely, if an integer divides both b and r, then it also divides a. It will then follow that g.c.d. $(a, b) =$ g.c.d. (b, r).

PROOF:

Suppose u divides a and b, i.e.,

$a = tu$ and $b = su$. Then, since

$a = bq + r$,

$r = a - bq = tu - suq$, or

$r = u(t - sq)$.

What does this statement prove?

ANSWER:

That u divides r.

Therefore, if an integer divides a and b, it also divides b and r. In a similar way, show that if an integer divides b and r, then it also divides a and b.

ANSWER:

Suppose w divides b and r, i.e.,

$b = tw$ and $r = sw$. Then, since

$a = bq + r$,

$a = twq + sw$,

or

$a = w(tq + s)$.

$\therefore$ w divides a and we have proved that if an integer w divides b and r, then it also divides a and b.

We will illustrate the usefulness of this relation between the divisors of a and b and the divisors of b and r by finding the greatest common divisor of 3806 and 1211. We divide 3806 by 1211 and put the results in the form $a = bq + r$, i.e., $3806 = (1211)(3) + 173$. Therefore g.c.d. (3806, 1211) = g.c.d. (1211, 173). The problem of finding g.c.d. (3806, 1211) has been replaced by a problem involving smaller numbers.

We divide 1211 by 173 and find that $1211 = 173(7) + 0$. Therefore g.c.d. (3806, 1211) = g.c.d. (1211, 173) = g.c.d. (173, 0) = 173. The greatest common divisor of 3806 and 1211 is 173.

Euclid's Algorithm is the name given to the process of finding the g.c.d. of two numbers that is based on Theorem 9.3. Algebraically we can describe the process as follows:

$$\begin{aligned} a &= bq_1 + r_1 & 0 &< r_1 < b \\ b &= r_1q_2 + r_2 & 0 &< r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 &< r_3 < r_2 \end{aligned}$$

What is the next step in the sequence? (Use same notational pattern.)

ANSWER:

$$r_2 = r_3q_4 + r_4 \qquad 0 < r_4 < r_3$$

This process is continued until a remainder of zero is obtained, i.e.,

$r_{n-2} = r_{n-1}q_n + r_n \qquad 0 < r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1} + 0 \qquad 0 = r_{n+1} < r_n.$

Thus g.c.d. $(a, b) =$ g.c.d. $(r_n, 0) = r_n$. r_n is the last nonzero remainder obtained.

The inequalities on the right can be combined to form a statement involving positive integers:

$|b| > r_1 > r_2 > \ldots > r_n > r_{n+1} = 0.$

What is an upper bound for the number of times that the division theorem could be applied before a remainder of zero is obtained?

ANSWER:

$|b|$ (There are just $|b|$ integers from 0 to $|b| - 1$ inclusive.)

If both a and b are zero, then every positive integer is a common divisor of a and b, hence there is no greatest common divisor. If either $a = 0$ or $b = 0$, say $b = 0$, what can be said about the g.c.d. (a, b) if $a > 0$? If $a < 0$?

ANSWER:

If $b = 0$ and $a > 0$, g.c.d. $(a, b) =$ g.c.d. $(a, 0) = a$;

If $b = 0$ and $a < 0$, g.c.d. $(a, b) =$ g.c.d. $(a, 0) = -a$.

Find the greatest common divisor of the following pair of integers by Euclid's Algorithm.

-729 and 378

ANSWER:

$-729 = 378 \cdot (-2) + 27$

$378 = 27 \cdot 14 + 0$

$\therefore$ g.c.d. $(-729, 378)$ = g.c.d. $(378, 27)$ = g.c.d. $(27, 0)$ = 27.

DEFINITION 9.4: Two integers that have no common divisors other than units are said to be relatively prime.

State the definition of unit given earlier in this section for the systems N and I.

ANSWER:

A unit is an element of a system that has a multiplicative inverse in the system.

Name the units in the system I.

ANSWER:

1 and -1.

THEOREM 9.4: If d = g.c.d. (a, b), where $a \neq 0$ and $b \neq 0$, then there exist integers k and ℓ such that $d = ka + \ell b$.

We restrict a and b to be non-zero, since if either a or b is zero, the theorem is trivial. For example, if $b = 0$, $a > 0$, then d = g.c.d. (a, b) = g.c.d. $(a, 0)$ $= a = 1 \cdot a + \ell \cdot 0$, where $k = 1$ and ℓ is any integer.

PROOF: Let S be the set of all positive integers of the form $ka + \ell b$. We wish to show d is in S. We know that S has a least element. Why?

ANSWER:

The positive integers are the natural numbers, and the natural numbers are well ordered; hence any subset of the positive integers has a least element.

Let s be the least element of S. Then there are integers k_1 and ℓ_1 such that $s = k_1a + \ell_1b$.

By Theorem 9.1,

$a = q_1s + r_1$, where $0 \leq r_1 < s$.

So

$r_1 = 1 \cdot a + (-q_1)s$.

Show that r_1 can be written in the form $ka + \ell b$, for some integers k and ℓ.

ANSWER:

$r_1 = 1 \cdot a + (-q_1)s = 1 \cdot a + (-q_1)(k_1a + \ell_1b) = (1 - q_1k_1)a + (-q_1\ell_1)b$, which is of the required form with $k = 1 - q_1k_1$ and $\ell = -q_1\ell_1$.

Looking again at the definition of the set S and recalling that s is the least element of S, what can you deduce from the conditions: $0 \leq r_1 < s$, and $r_1 = ka + \ell b$ for integers a and b?

ANSWER:

$r_1 = 0$. If $r_1 > 0$ then r_1 is a positive integer and is in S. But r_1 cannot be in S because it is less than the least element of S.

Since $r_1 = 0$, $a = q_1 s$. Therefore s is a divisor of a. In a similar way show that s is a divisor of b.

ANSWER:

By Theorem 9.1,

$$b = q_2 s + r_2, \quad \text{where} \quad 0 \leq r_2 < s.$$

So

$$\begin{aligned} r_2 &= 1 \cdot b + (-q_2)s = 1 \cdot b + (-q_2)(k_1 a + \ell_1 b) \\ &= (-q_2 k_1)a + (1 - q_2 \ell_1)b. \end{aligned}$$

Therefore r_2 can be expressed in the form $ka + \ell b$, with integers k and ℓ. If $r_2 > 0$ then r_2 is a positive integer and is in S. But r_2 cannot be in S because it is less than the least integer in S. So $r_2 = 0$. Therefore $b = q_2 s$, and s is a divisor of b.

We have shown that s is a common divisor of a and b. Why can we conclude that $s \leq d$, where d = g.c.d. (a, b)?

ANSWER:

Because s is a common divisor and d is the greatest common divisor of a and b.

Show that d is a divisor of $s = k_1a + \ell_1b$.

ANSWER:

Since d is a common divisor of a and b, we can write $a = md$, $b = nd$, where m and n are integers. Then

$s = k_1a + \ell_1b = k_1md + \ell_1nd = (k_1m + \ell_1n)d$. So d is a divisor of s.

Since d is a divisor of s, we conclude that $d \leq s$. But we have previously shown that $s \leq d$. What can we conclude?

ANSWER:

$s = d$.

This proves that d can be expressed in the form $ka + \ell b$ and completes the proof of Theorem 9.4.

We have actually proved that d not only can be expressed in the form $ka + \ell b$, but is the least positive integer which can be expressed in that form. An integer of the form $ka + \ell b$ is called a sum of multiples of a and b.

We have seen earlier how to find d, the g.c.d. of integers a and b, by Euclid's Algorithm. The process can also be used to find integers k and ℓ such that $d = ka + \ell b$. We will illustrate with an example.

Find $d =$ g.c.d. (228, 177) by Euclid's Algorithm.

ANSWER:

$228 = 177 \cdot 1 + 51$

$177 = 51 \cdot 3 + 24$

$51 = 24 \cdot 2 + 3$

$24 = 3 \cdot 8 + 0$

$\therefore$ g.c.d. $(228, 177) =$ g.c.d. $(3, 0) = 3$.

We wish to find integers k and ℓ such that $3 = k \cdot 228 + \ell \cdot 177$. Using the equations above:

$3 = 51 - 2 \cdot 24$

$24 = 177 - 3 \cdot 51$

$51 = \underline{\qquad}$

ANSWER:

$51 = 228 - 177$

$$\begin{aligned} \text{Thus } 3 &= 51 - 2 \cdot 24 \\ &= 51 - 2(177 - 3 \cdot 51) \\ &= 7 \cdot 51 - 2 \cdot 177 \\ &= 7(228 - 177) - 2 \cdot 177 \\ &= 7 \cdot 228 - 9 \cdot 177. \end{aligned}$$

$\therefore k = \underline{\qquad}$ and $\ell = \underline{\qquad}$

ANSWER:

7

-9

(a) Find $d = \text{g.c.d.}\ (117, 91)$, and then

(b) Find integers k and ℓ such that $d = k \cdot 117 + \ell \cdot 91$.

ANSWER:

(a)
$$117 = 91 \cdot 1 + 26$$
$$91 = 26 \cdot 3 + 13$$
$$26 = 13 \cdot 2 + 0$$

$\therefore$ g.c.d. $(117, 91)$ = g.c.d. $(13, 0) = 13$.

(b) $k = -3$ and $\ell = 4$. This is shown as follows:

from (a) above,
$$13 = 91 - 3 \cdot 26$$
$$26 = 117 - 91$$
$$\therefore \quad 13 = 91 - 3(117 - 91)$$
$$\text{or} \quad 13 = -3 \cdot 117 + 4 \cdot 91$$

Theorem 9.4 enables us to prove the uniqueness part of the fundamental theorem of arithmetic (unique factorization) in a manner different from and independent of that used in the section on natural numbers. This illustrates that there is often more than one way to prove a mathematical theorem. In the present proof, we first prove as a lemma the theorem that was previously stated as a corollary to the fundamental theorem of arithmetic.

Lemma: (Corollary 1 of Theorem 8.8): If a prime p is a factor of ab, then p must be a factor of either a or b.

PROOF: The hypothesis states that p is a factor of ab or $ab = pr$. If p is a factor of a, there is nothing to prove. Assume p is not a factor of a, i.e., g.c.d. $(a, p) = 1$. Then we must prove p is a factor of b.

From g.c.d. $(a, p) = 1$, we have

(1) $1 = ka + \ell p$, for some integers k and ℓ. Why?

ANSWER:

Theorem 8.4.

Multiply both sides of equation (1) by b, then show that p is a factor of b.

ANSWER:

$b = kab + \ell pb$ and, by hypothesis, $ab = pr$. Thus

$b = kpr + \ell pb = (kr + \ell b)p$

from which it is evident that p is a factor of b.

Note that the lemma can be extended by induction to show that if p is a divisor of a product of any number of factors, then p must be a divisor of one of the factors of the product.

The uniqueness part of the fundamental theorem of arithmetic (Theorem 8.8) follows from this lemma. The following proof would involve induction if it were to be made completely rigorous.

We assume, as before, that some n in N has two prime factorizations, $n = p_1 \cdot p_2 \cdots p_\ell = q_1 \cdot q_2 \cdots q_m$. Since p_1 divides the left side of this equation it must also divide the right. Moreover the lemma tells us that it must divide one of the factors. q_k, of the right. If p_1 divides q_k then $p_1 = q_k$. Why?

ANSWER:

$p_1 = q_k$ because q_k is prime.

Therefore we can cancel these equal factors from the equation.

In like manner, we can show that p_2 is a factor of some q_j and therefore $p_2 = q_j$. We can continue this process with $p_3, \ldots, p_\ell$ until all of the p's are cancelled. What is the left hand side equal to after this cancellation?

- -

ANSWER:

One.

- -

How many q's remain on the right side? Why?

- -

ANSWER:

None; since $p_1 \cdot p_2 \cdots p_\ell = q_1 \cdot q_2 \cdots q_m$ and since all the p's have been cancelled, the product on the left is 1. But then the product on the right is also 1, and since no $q_j = 1$, $(j = 1, 2, \ldots m)$, then all the q's have been cancelled.

- -

Therefore the p's and q's have been paired into equal couples and the two decompositions are the same except for the order of the factors.

- -

PRIME INTEGERS

Recall the definition of a prime natural number. A natural number p is said to be prime if ____.

- -

ANSWER:

$p > 1$ and p cannot be written as the product of two natural numbers other than p and 1.

- -

A natural number c is said to be composite if ____.

- -

ANSWER:

$c > 1$ and c is not prime.

- -

DEFINITION 9.5: A positive integer is prime if and only if it is a prime natural number. A negative integer is prime if and only if its additive inverse is a prime natural number. The integers 1, -1, and 0 are neither prime nor composite. All other integers (except the primes and the numbers 1, -1, and 0) are composite.

Which of the following integers are prime integers?

97, -67, -1, -93, 89, 197.

- -

ANSWER:

97, -67, 89, 197.

- -

DEFINITION 9.6: By standard factorization of an integer we mean a factorization containing as factors only positive prime integers and a unit (either 1 or -1).

Every composite or prime integer has a unique standard factorization.

The standard factorization of 12 is $1 \cdot 2^2 \cdot 3$. The standard factorization of -7 is $(-1) \cdot 7$.

Find the standard factorization of the following integers:

(a) 78

- -

ANSWER:

$1 \cdot 2 \cdot 3 \cdot 13$.

(b) -258

ANSWER:

$(-1) \cdot 2 \cdot 3 \cdot 43$

COUNTABILITY

Recall the definition of countable. We say that a non-empty set S is countable if there is a reversible function f whose domain is the set ____ and whose range is the set ____.

ANSWER:

of natural numbers

S.

Let f be the function defined by

$f(n) = n/2$, for each even natural number n.

Then f: $2 \rightarrow 1$

$4 \rightarrow 2$

$6 \rightarrow 3$

etc.

f is a function from the set ____ onto the set ____.

ANSWER:

of even natural numbers

of natural numbers.

Give a rule for a function f from the set of odd natural numbers onto the set of negative integers and 0. [Hint: Choose f such that f: $1 \to 0$; $3 \to -1$; $5 \to -2$, etc.]

ANSWER:

$f(n) = -(\frac{n-1}{2})$, for each odd natural number n.

If we define f on the set of natural numbers by

$f(n) = n/2$, when n is even

$f(n) = -(\frac{n-1}{2})$, when n is odd,

then it can be shown that f is a reversible function from the set N onto the set I. This would show that the set I is ____.

ANSWER:

countable.

REVIEW ITEMS

1. List each field postulate which is not valid for the system of integers.

ANSWER:

M_{in}.

---

2. (a) Find the standard factorization of 1463.

- -

ANSWER:

$1 \cdot 7 \cdot 11 \cdot 19$.

- -

(b) Find the standard factorization of -1197

- -

ANSWER:

$(-1) \cdot 3 \cdot 3 \cdot 7 \cdot 19$

- -

(c) What is the g.c.d. (1463, -399)?

- -

ANSWER:

$7 \cdot 19$ or 133.

- -

3. Use the Euclidean Algorithm to find the g.c.d. (119, 85). Show your work.

- -

ANSWER:

$119 = 85 \cdot 1 + 34$

$85 = 34 \cdot 2 + 17$

$34 = 17 \cdot 2 + 0$

$\therefore$ g.c.d. (119, 85) = g.c.d. (85, 34) = g.c.d. (34, 17) = g.c.d. (17, 0) = 17

- -

4. Use the equations in your preceding answer to find integers k and ℓ such that $17 = k \cdot 119 + \ell \cdot 85$.

ANSWER:

$k = -2$ and $\ell = 3$. These are obtained as follows:

$$\begin{aligned} 17 &= 85 - 2 \cdot 34 \\ &= 85 - 2(119 - 85) \\ &= 3 \cdot 85 - 2 \cdot 119 \end{aligned}$$

5. Which of the following subsets of I are closed under addition?

(a) The set of positive integers.

(b) The set of negative integers.

(c) The odd integers.

(d) The set of integers of the form $a \cdot 10^n$, where a is an integer and n is a natural number.

ANSWER:

(a)

(b)

(d).

6. Which of the above sets are closed under multiplication?

ANSWER:

(a)

(c)

(d).

7. Define a function to show that the set of odd integers (positive and negative) is countable.

ANSWER:

$1 \xrightarrow{f} 1$

$2 \longrightarrow -1$

$3 \longrightarrow 3$

$4 \longrightarrow -3$

. .

. .

. .

$n \longrightarrow n$ if n is an odd natural number.

$n \longrightarrow -n + 1$ if n is an even natural number.

. .

. .

. .

Or, the function f such that $n \xrightarrow{f} n$ if n is an odd natural number, and $n \xrightarrow{f} -n + 1$ if n is an even natural number.

---

8. Perform the following divisions and state the results in the form $a = bq + r$, where $0 \leq r < |b|$.

(a) Divide -249 by 19.

ANSWER:

$-249 = 19 \cdot (-14) + 17$ (Remember, r must be non-negative.)

(b) Divide -187 by -15.

ANSWER:

$-187 = (-15)(13) + 8$

---

9. Express 119 (base ten) in base three as an expanded numeral and as a numeral.

ANSWER:

$119 = 2 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + 1 \cdot 3^4$

[illegible]d 119 (base ten) = 11102 (base three).

---

10. Two integers such as 27 and 10, which have no common factors other than 1 or -1, are said to be ____.

ANSWER:

relatively prime.

X. RATIONAL NUMBERS

DEFINITION OF THE SET Q

Another subset of the set of real numbers that deserves special attention is the system of rational numbers. We will show that the set of rational numbers satisfies all the postulates for a field and that it is the smallest subset of R which contains the integers and which, with real number addition and muitiplication, forms a field. We will also list some properties possessed by the set of rational numbers that distinguish that set from the other sets of numbers previously discussed.

We will denote the set of rational numbers by "Q".

DEFINITION 10.1: The set of rational numbers, Q, is the set of all real numbers which are quotients of integers; i.e., a real number q is rational if and only if $q = a \div b = a/b$, where a and b are integers and $b \neq 0$.

Are integers rational numbers; i.e., can an integer be expressed as the ratio of two integers? Why?

- -

ANSWER:

Yes; if n is an integer, then $n = n \cdot 1 = n \cdot 1^{-1} = n/1$.

- -

The choice of the word "rational" for this set of numbers is a reasonable one, since a rational number is defined in terms of the quotient of "ratio" of two integers.

In order to determine when two fractions represent the same rational number, we first recall that if a, b, c, d are real numbers ($b, d \neq 0$), then $a/b = c/d$ if and only if $ad = bc$. (Theorem 3.15).

Using the above theorem, how would you decide whether or not $-7/13$ and $119/-221$ are equal?

ANSWER:

By comparing the products $(-7) \cdot (-221)$ and $(13) \cdot (119)$. Since both products equal 1547, $-7/13$ and $119/-221$ are equal.

DEFINITION 10.2: A fraction a/b, where a and b are integers ($b \neq 0$), is said to be in lowest terms if a and b have no common divisors except 1 and -1, and b is positive.

Which of the following fractions are in lowest terms?

(a) $42/91$

(b) $-21/46$

(c) $35/-51$

ANSWER:

(b) $-21/46$

OPERATIONS AND THEIR PROPERTIES

Since the operations of real number addition and multiplication are closed, the sum or product of any two real numbers is a(n) ____.

ANSWER:

real number.

Therefore, if a/b and c/d are any two rational numbers, their sum and product are ____. To prove closure of rational number addition and multiplication, we must show that the sum and product of any two rational numbers are ____.

- -

ANSWER:
real numbers.
rational numbers.

- -

With Theorems 3.11 and 3.13, we can prove that rational number addition and multiplication are closed. Suppose a, b, c, d are integers, $b, d \neq 0$, then

$$a/b + c/d = \frac{ad + bc}{bd} \qquad (bd \neq 0)$$

by Theorem 3.11. Why can we conclude that $a/b + c/d$ is a rational number?

- -

ANSWER:
By the closure of addition and multiplication of integers, $ad + bc$ and bd are integers. Hence $\frac{ad + bc}{bd}$ is a rational number, by Definition 10.1.

- -

This proves that rational number addition is closed.

Prove that rational number multiplication is closed.

- -

ANSWER:
Suppose a, b, c, d are integers, $b, d \neq 0$, then $a/b \cdot c/d = ac/bd$ $(bd \neq 0)$ by Theorem 3.13. By the closure of multiplication of integers, ac and bd are integers. Hence ac/bd is a rational number, by Definition 10.1.

Do the commutative laws hold for addition and multiplication in Q; i.e., if a and b are rational numbers, do $a + b = b + a$ and $a \cdot b = b \cdot a$ hold? Explain.

ANSWER:

Yes; a and b are real numbers, and the commutative laws hold for real number addition and multiplication.

Do the associative laws hold for the operations in Q; i.e., if a, b, c are rational numbers, do $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ hold? Explain.

ANSWER:

Yes; a, b, c are real numbers and the associative laws hold for real number addition and multiplication.

State the distributive law for the operations in Q. Is it valid in Q?

ANSWER:

If a, b, c are rational numbers, then $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$. Yes.

What remaining field properties must the system Q possess in order that it be a field?

ANSWER:

A_{id}, A_{in}, M_{id}, and M_{in} properties.

Are 0 and 1 in Q? Why?

ANSWER:

Yes; 0 and 1 are integers, and the set Q contains all the integers.

If a is any rational number, does a + 0 = 0 + a = a? Why?

ANSWER:

Yes; a is a real number and 0 is the additive identity in the set of real numbers, hence 0 is the additive identity for Q.

If a is a rational number, does a · 1 = 1 · a = a for every a in Q? Why?

ANSWER:

Yes; a is a real number and 1 is the identity element for multiplication in R, hence 1 is the multiplicative identity for Q.

If a is a rational number, does the additive inverse of a exist in R? Why?

ANSWER:

Yes; a is a real number, and the A_{in} postulate guarantees the existence of the additive inverse of a for every a in R.

Does this prove that Q has the A_{in} property? Why?

- -

ANSWER:

No; we must prove that if a is a rational number, the additive inverse of a is a rational number.

- -

Let $a = p/q$, where p and q are integers $(q \neq 0)$. Then $-a = -p/q$. Is $-p/q$ a rational number?

- -

ANSWER:

Yes.

- -

If a is any non-zero rational number, does the multiplicative inverse of a exist in R? Why?

- -

ANSWER:

Yes; a is a non-zero real number, and the M_{in} postulate guarantees the existence of the multiplicative inverse of a for every non-zero a in R.

- -

What must be done to prove that Q has the M_{in} property?

- -

ANSWER:

We must prove that if a is a non-zero rational number, the multiplicative inverse of a is a rational number.

- -

Let a = p/q, where p and q are any two non-zero integers. Thus p/q is a rational number by Definition 10.1. The multiplicative inverse of p/q is ____.

- -

ANSWER:

q/p.

- -

q/p is a rational number since p and q are non-zero integers.

We have shown that Q possesses all the basic field properties; i.e., closure under addition and multiplication, A_c, M_c, A_a, M_a, A_{id}, M_{id}, A_{in}, M_{in}, and D. Thus Q, a subset of R, is a field under the operations in R restricted to Q. Therefore, we say Q is a subfield of R.

Since Q satisfies the field postulates, subtraction and division (except by zero) are closed operations in Q.

To show that Q is the smallest subfield of R containing the integers, we note that any subfield, A, of R containing the integers must also contain the multiplicative inverse of each non-zero integer and must be closed under multiplication. Thus if a and b are any two integers in A, b ≠ 0, then b^{-1} must be in A, and $a \cdot b^{-1}$ must be in A. But if A contains ab^{-1} for every pair of integers a, b (b ≠ 0), then Q is a subset of A, by definition of the set Q. Hence Q is the smallest subfield of R containing the integers.

Actually, it is not difficult to see that every subfield of R must contain the integers, and hence must contain Q. We will not prove this here.

ORDER

Since the order postulates 01, 02, 03, 04 as stated for the real numbers do not require the existence of any special elements in R, they hold equally well for the set of rational numbers because rational numbers are real numbers. That is, from O1, we have "if a and b are any real numbers, then one and only one of the following is true, $a < b$, $a = b$, $a > b$". Thus if a and b are rational numbers, property O1 applies since rational numbers are real numbers. Similarly, the properties O2, O3, and O4 hold for Q.

Using Order Theorem 4.20, we can reduce the problem of determining which of two rational numbers is greater to that of determining which of two integers is greater. For example, suppose we have to decide which of two rational numbers, $7/22$ or $34/111$, is greater. The answer is not immediately apparent. We note that since $7 \cdot 111 > 22 \cdot 34$ (or $777 > 748$), then $34/111$ ____ $7/22$ (insert < or >).

ANSWER:

<

Thus the relative order of any two rational numbers can be determined by comparison of integers, for if a, b, c, d in Order Theorem 4.20 are integers ($b > 0$, $d > 0$), then ad and bc are integers and $a/b > c/d$ if and only if $ad > bc$.

Consider the following statement:

If $7/-11 > -9/13$, then $7 \cdot 13 > (-11) \cdot (-9)$.

Is the above statement true or false?

ANSWER:

False; $7/-11$ is greater than $-9/13$, but $7 \cdot 13 \not> (-11)(-9)$.

Why does Theorem 4.20 fail to apply in this example?

ANSWER:

The denominator of the fraction $7/-11$ is negative, whereas in Theorem 4.20 the denominator was required to be positive. Note that if the rational number a/b has b negative, we can write $a/b = -a/-b$, where $(-b)$ is a positive number.

- -

What change in the preceding example would permit us to apply Theorem 4.20?

- -

ANSWER:

Multiply numerator and denominator of the fraction $7/-11$ by -1, obtaining $-7/11$.

- -

If $-7/11 > -9/13$, then $(-7) \cdot (13) > (11) \cdot (-9)$. Is this statement true or false?

- -

ANSWER:

True; (Theorem 4.20 now applies, and -91 is greater than -99.)

- -

Which is greater, $-5/17$ or $-7/19$? Why?

- -

ANSWER:

$-5/17$; because $(-5) \cdot (19) > (17) \cdot (-7)$ or, $-95 > -119$.

- -

PROPERTIES OF THE SYSTEM OF RATIONAL NUMBERS

We now list some properties of the set of rational numbers as compared to the other sets of numbers previously discussed.

The set of rational numbers is closed under the operations of addition, subtraction, multiplication, and division (except by zero). Recall that the set of integers is not closed under ____, and the set of natural numbers is not closed under ____.

- -

ANSWER:

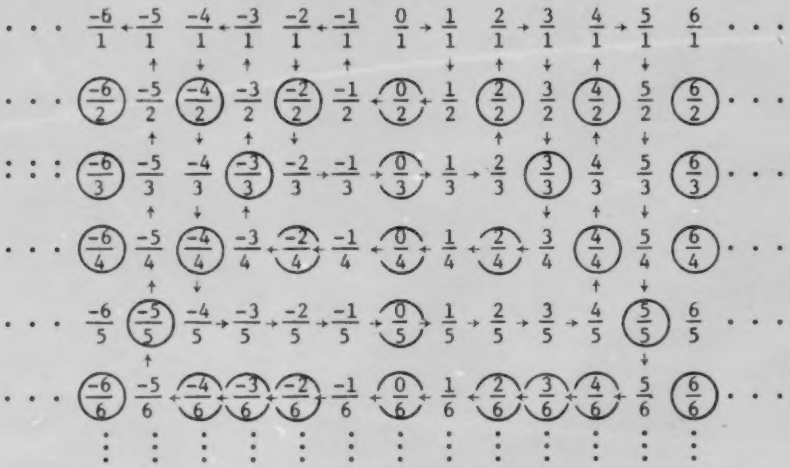
division,

subtraction and division.

- -

The set Q is countable. That is, the rational numbers can be placed in one-to-one correspondence with the natural numbers. This is also a property of the set of integers.

To show that the set of rational numbers is countable, consider the following infinite array of rational numbers which guarantees that every rational number is contained somewhere within the array. The top row contains all fractions of integers with denominator 1. The second row contains all fractions of integers with denominator 2. The third row contains all fractions of integers with denominator 3, etc.



. . . -6/1 -5/1 -4/1 -3/1 -2/1 -1/1 0/1 1/1 2/1 3/1 4/1 5/1 6/1 . . .
. . . -6/2 -5/2 -4/2 -3/2 -2/2 -1/2 0/2 1/2 2/2 3/2 4/2 5/2 6/2 . . .
. . . -6/3 -5/3 -4/3 -3/3 -2/3 -1/3 0/3 1/3 2/3 3/3 4/3 5/3 6/3 . . .
. . . -6/4 -5/4 -4/4 -3/4 -2/4 -1/4 0/4 1/4 2/4 3/4 4/4 5/4 6/4 . . .
. . . -6/5 -5/5 -4/5 -3/5 -2/5 -1/5 0/5 1/5 2/5 3/5 4/5 5/5 6/5 . . .
. . . -6/6 -5/6 -4/6 -3/6 -2/6 -1/6 0/6 1/6 2/6 3/6 4/6 5/6 6/6 . . .

By starting with 0/1, and following a system of counting as indicated by the arrows, we are assured that every rational number will be counted. The above illustration shows how the rational numbers can be placed in one-to-one correspondence with the natural numbers. Note that those rational numbers that are circled in the array are not put into this correspondence since they have previously been counted. For example, 0/2 is not put into this correspondence because 0/2 = 0 = 0/1, which has already been counted.

N   Q
1 ⟶ 0/1
2 ⟶ 1/1
3 ⟶ 1/2
4 ⟶ -1/2
5 ⟶ -1/1
6 ⟶ -2/1
7 ⟶ -2/3
8 ⟶ -1/3
9 ⟶ 1/3
10 ⟶ 2/3
11 ⟶ 2/1
12 ⟶ 3/1
.   .
.   .
.   .

Continuing this scheme, what rational numbers will correspond to the following natural numbers?

15 ⟶
20 ⟶
33 ⟶
46 ⟶

- -

ANSWER:

15 ⟶ 1/4

20 ⟶ -4/1

33 ⟶ 5/2

46 ⟶ -6/7

The set of real numbers is not countable but we will not prove this here.

The rational numbers can be represented by decimals. To every rational number there corresponds a decimal that either terminates or, if non-terminating, is periodic in the sense that a certain set of digits is repeated. For example, in converting the rational number 43/8 to a decimal, we have, by the division algorithm,

(1) $43 = 8 \cdot 5 + 3$, and so 5 is the integral (whole number) part of the decimal representation. Multiplying the remainder by 10, we have

(2) $30 = 8 \cdot 3 + 6$, and 3 is the first digit after the decimal point. We now multiply the second remainder by 10 obtaining

(3) $60 = 8 \cdot 7 + 4$. Thus 7 is the second digit after the decimal point. Multiplying the third remainder by 10 we have

(4) $40 = 8 \cdot 5$, and 5 is therefore the third and final digit after the decimal point.

We show this by taking the equations above in reverse order, dividing by 10, and substituting in the preceding equation. Hence from (4) $4 = 8 \cdot 5/10$ and from (3), $60 = 8 \cdot 7 + 8 \cdot 5/10$ or $6 = 8 \cdot 7/10 + 8 \cdot 5/10^2$.

Substitute this last expression in equation (2), divide by 10, and show the result.

ANSWER:

From (2), $30 = 8 \cdot 3 + 8 \cdot 7/10 + 8 \cdot 5/10^2$

or $3 = 8 \cdot 3/10 + 8 \cdot 7/10^2 + 8 \cdot 5/10^3$

- -

Substitute this last expression in equation (1), and show the result.

- -

ANSWER:

From (1), $43 = 8 \cdot 5 + 8 \cdot 3/10 + 8 \cdot 7/10^2 + 8 \cdot 5/10^3$

- -

Dividing this last result by 8, we have

$43/8 = 5 + 3/10 + 7/10^2 + 5/10^3 = 5.375$

To convert any rational number a/b (where a/b is not an integer) into a decimal we proceed in the same way. Assume a and b positive. We have, by the division algorithm,

(1) $a = b \cdot q + r_0$, where $0 < r_0 < b$, and q is the integral part of a/b.

(2) $10r_0 = b \cdot q_1 + r_1$, where $0 \leq r_1 < b$.

Show that $q_1 < 10$. (You need not list theorems and postulates as reasons. Simply give the basic steps of a proof.)

- -

ANSWER:

Since $r_0 < b$, $10r_0 < 10b$. Then $bq_1 + r_1 < 10b$. Because $r_1 \geq 0$, $bq_1 \leq bq_1 + r_1 < 10b$. Then $q_1 < 10$.

- -

q_1 is the first digit after the decimal point. From equation (2) we have

$r_0 = b \cdot q_1/10 + r_1/10$,

and from (1) we have

$a = b \cdot q + b \cdot q_1/10 + r_1/10.$

Then

(3) $a/b = q + q_1/10 + r_1/10b.$

If $r_1 = 0$,

$a/b = q + q_1/10 = q.q_1.$

If $r_1 \neq 0$, we continue, obtaining

(4) $10r_1 = b \cdot q_2 + r_2 , \quad 0 \leq r_2 < b.$

As before, we can show that $q_2 < 10$. Therefore, q_2 is the second digit after the decimal point.

Show that equations (3) and (4) imply

$a/b = q + q_1/10 + q_2/10^2 + r_2/10^2b$

- -

ANSWER:

By (4), $r_1/b = q_2/10 + r_2/10b.$

Substituting in (3), we get $a/b = q + q_1/10 + q_2/10^2 + r_2/10^2b.$

- -

If, in this last expression, $r_2 = 0$, the decimal terminates and $a/b = q + q_1/10 + q_2/10^2 = q.q_1q_2$. If $r \neq 0$, we continue as before until some $r_n = 0$, in which case the decimal terminates, and

$a/b = q + q_1/10 + q_2/10^2 + \ldots + q_n/10^n = q.q_1q_2 \cdots q_n.$

If no $r_n = 0$, then, since $0 \leq r_n < b$, in no more than b divisions one of the remainders previously encountered must occur again, and the decimal repeats.

What are the possible remainders when dividing a by b?

- -

ANSWER:

$0, 1, 2, 3, \ldots, b - 1.$

- -

Thus, if $r_n \neq 0$, there are only $b - 1$ positive integers from 1 to $b - 1$, hence on the b^{th} division, one of the previous remainders must occur a second time. Of course, a remainder may occur for the second time before the b^{th} division.

Let us illustrate with another example. We divide 51 by 37; i.e., we take $a = 51$, $b = 37$.

$$51 = 37 \cdot 1 + 14 \qquad q = 1, \quad r_0 = 14$$

$$51/37 = 1 + 14/37$$

$$10 \cdot 14 = 140 = 37 \cdot 3 + 29 \qquad q_1 = 3, \quad r_1 = 29$$

Then

$$14/37 = 3/10 + \frac{29}{10 \cdot 37},$$

and

$$51/37 = 1 + 3/10 + \frac{29}{10 \cdot 37}.$$

Next

$$10 \cdot 29 = 290 = 37 \cdot 7 + 31. \qquad q_2 = 7, \quad r_2 = 31$$

Then

$$29/37 = 7/10 + \frac{31}{10 \cdot 37},$$

and

$$51/37 = 1 + 3/10 + 7/10^2 + \frac{31}{10^2 \cdot 37}.$$

Next

$$10 \cdot 31 = 310 = 37 \cdot 8 + 14. \qquad q_3 = 8, \quad r_3 = 14$$

Then

$$31/37 = 8/10 + \frac{14}{10 \cdot 37},$$

and

$51/37 = 1 + 3/10 + 7/10^2 + 8/10^3 + 1/10^3 \cdot 14/37$

Since $r_3 = r_0 = 14$, the decimal repeats as follows:

$51/37 = 1.378378\overline{378}$. (The bar over 378 indicates that the sequence of digits repeats.)

Find the digits $q, q_1, q_2, \ldots$ and the remainders $r_0, r_1, r_2, \ldots$ up to the point where repetition begins when 17 is divided by 7.

- -

ANSWER:

$$\begin{array}{rcllcl} 17 & = & 7 \cdot 2 + 3 & q = 2, & r_0 = 3 \\ 10 \cdot 3 & = & 7 \cdot 4 + 2 & q_1 = 4, & r_1 = 2 \\ 10 \cdot 2 & = & 7 \cdot 2 + 6 & q_2 = 2, & r_2 = 6 \\ 10 \cdot 6 & = & 7 \cdot 8 + 4 & q_3 = 8, & r_3 = 4 \\ 10 \cdot 4 & = & 7 \cdot 5 + 5 & q_4 = 5, & r_4 = 5 \\ 10 \cdot 5 & = & 7 \cdot 7 + 1 & q_5 = 7, & r_5 = 1 \\ 10 \cdot 1 & = & 7 \cdot 1 + 3 & q_6 = 1, & r_6 = 3 \end{array}$$

Here $r_6 = r_0 = 3$, and the decimal repeats. Then $17/7 = 2.428571\overline{428571}$.

- -

Note: In the preceding we have assumed that the division process does generate the decimal expansion of the given rational number. This requires proof in the case where the process does not terminate, but we will not give a proof here.

If a decimal terminates, it can be represented as a quotient of an integer and some non-negative power of 10, hence it is a rational number. Convert the terminating decimal 1.247 to a quotient of integers.

- -

ANSWER:

$$1.247 = \frac{1247}{10^3} = \frac{1247}{1000}$$

- -

To illustrate how a non-terminating, repeating decimal represents a rational number, consider the following examples. (A rigorous proof involves the least upper bound idea and is beyond the scope of this course.)

Let $x = .4545\overline{45}$ where $\overline{45}$ indicates that the digits 4, 5 are repeated indefinitely.

Then $100x = 45.4545\overline{45} = 45 + x$

Note that this step is obtained by multiplying both sides of the previous equation by 10^n, where n is the number of digits repeated in the decimal. (In this case $n = 2$.)

and $99x =$ ____ .

or $x =$ ____.

- -

ANSWER:

45

45/99 = 5/11.

- -

As another illustration, let

$x = 1.4306306\overline{306}$

which can be written as

$x = 1 + 4/10 + N/10$, where

$N = .306306\overline{306}$

$1000N = 306.306306\overline{306} = 306 + N$

$999N =$ ____

$N =$ ____.

- -

ANSWER:

306

$\frac{306}{999} = \frac{34}{111}$

Hence $x = 1 + 4/10 + 34/1110 = 794/555$.

Convert the repeating decimal $.2108\overline{108}$ to a fraction of integers in lowest terms.

ANSWER:

Let $x = .2108\overline{108}$, which can be written as

$$
\begin{aligned}
x &= 2/10 + N/10, \quad \text{where } N = .108\overline{108}. \\
1000N &= 108.108\overline{108} = 108 + N \\
999N &= 108 \\
N &= 108/999 = 4/37 \\
x &= 2/10 + 4/370 = 78/370 = 39/185
\end{aligned}
$$

Suppose a and b are positive integers, $a < b$, and that a and b are relatively prime, so that a/b is in lowest terms. If we also assume that b is relatively prime to 10, then it can be shown that

$$a/b = .a_1a_2a_3 \ldots a_n\overline{a_1a_2a_3 \ldots a_n}.$$

a/b is a repeating decimal and the repeating sequence of digits begins with the first digit following the decimal point.

Then

$$10^n \cdot a/b = a_1a_2a_3 \ldots a_n + a/b$$

or

$$(10^n - 1)a = (a_1a_2a_3 \ldots a_n)b.$$

This equation implies that b is a factor of $(10^n - 1)a$. Since b and a are relatively prime, b is a factor of $10^n - 1$. Thus, if the fraction a/b, when converted to a decimal, repeats one digit, then the denominator of the fraction must be a divisor of $10^1 - 1 = 9$; i.e., b must equal 3 or 9. Similarly, if the fraction a/b repeats two digits when converted to a decimal, its denominator must be a divisor of ____.

- -

ANSWER:

99.

- -

Thus the only fractions whose decimals repeat two digits are those with denominators of ____.

- -

ANSWER:

11, 33, or 99. (Note that 3 and 9 are divisors of 99, but fractions with 3 or 9 in the denominator repeat one digit when converted to a decimal. Of course, we could say they repeat two digits, with both digits being the same!)

- -

What are the possible denominators of a fraction if it is to repeat three digits when converted to a decimal? (As before, assume that a and b are relatively prime, $a < b$, and b and 10 are relatively prime.)

- -

ANSWER:

27, 37, 111, 333, 999.

- -

COMPLETENESS AND THE RATIONAL NUMBERS

Briefly review the definitions of upper bound and least upper bound and the Completeness Postulate given in Unit VII.

Consider the set $A = \{n \mid n \text{ is a natural number and } n < 10\}$.

(1) Name an upper bound for A in the set of natural numbers N.

(2) Does A have a least upper bound in N? If so, what is it?

ANSWER:

(1) 9 (or any natural number larger than 9)

(2) Yes; 9.

Let $B = \{x \mid x \text{ is an integer and } x < 7\}$.

(1) List three upper bounds for B in the set of integers.

(2) List the least upper bound if there is one.

ANSWER:

(1) 6, 7, 8 (or any larger integers).

(2) 6.

We will prove later that there is no rational number whose square is 2; hence the real number $\sqrt{2}$ is irrational.

Consider the set S of all rational numbers x such that $x^2 < 2$. (In the following, Q is the set of rational numbers.)

(1) S is a non-empty set. List at least 2 of its members.

(2) S has an upper bound in Q. List one.

(3) S has a least upper bound. What is it?

(4) Is the least upper bound in Q?

ANSWER:

(1) For example, 1, 1/2.

(2) For example, 2.

(3) $\sqrt{2}$

(4) No, $\sqrt{2}$ is irrational.

Now let S be the set of all real numbers x such that $x^2 < 2$.

(1) List 2 members of S.

(2) List an upper bound of S in the set of real numbers.

(3) What is the least upper bound of S?

(4) Is the least upper bound in the set of real numbers?

ANSWER:

(1) 1, 1/2 (or any real numbers less than $\sqrt{2}$ and greater than $-\sqrt{2}$).

(2) The answer may be any real number x such that $x \geq \sqrt{2}$.

(3) $\sqrt{2}$

(4) Yes.

The above discussion suggests a basic difference between the rational number system and the real number system. The Completeness Postulate, valid for the real number system, is not valid for Q because the set $S = \{x \mid x^2 < 2,\ x \text{ rational}\}$ is a subset of Q which has an upper bound in Q but has no least upper bound in Q.

Could you use the set $S = \{x \mid x^2 < 4,\ x \text{ rational}\}$ as an example to show that the set of rational numbers does not satisfy the Completeness Property? Explain.

ANSWER:

No. In this example the least upper bound, 2, is in the set of rational numbers. This does not prove that the set of rational numbers is not complete.

- -

Consider the set S of rational numbers x such that $x < 2\pi$. (Note: 2π is an irrational number.)

(1) Does S have an upper bound in the set of rational numbers?

(2) What is the least upper bound of S?

(3) Can this serve as an example to show that the Completeness Property does not hold for the system of rational numbers? Explain.

- -

ANSWER:

(1) Yes.

(2) 2π

(3) Yes, there is an upper bound for S in the set of rational numbers, but the least upper bound 2π is not an element of the set of rational numbers.

- -

If the following sets of real numbers have upper bounds, name the least upper bound. Decide in each case whether the l.u.b. is in the set of rational numbers.

(1) $S = \{x \mid x^2 \leq 3\}$

(2) $S = \{x \mid 0 < x < 9\}$

(3) $S = \{-1, 0, 1\}$

(4) The set of all even integers.

- -

ANSWER:

(1) $\sqrt{3}$ (not an element of the set of rational numbers).

(2) 9 (rational).

(3) 1 (rational).

(4) This set has no upper bound.

- -

COMPARISON OF SYSTEMS OF NUMBERS

We have, throughout this course, placed considerable emphasis on the field properties of the real numbers. In this and the preceding two units, we have considered three sub-systems of the reals and have shown precisely which of the field postulates are possessed by each of the sets N, I, and Q. As remarked earlier in the course, an alternative method for studying the real numbers is to begin with the system of natural numbers and certain basic properties of this system as axioms. Then one constructs, or builds, from the natural numbers the integers, the rational numbers, and finally the real numbers. Historically, this is approximately the way the number system was developed, although the positive rational numbers were in use long before the negative integers.

To summarize our development of the subsystems of the reals with regard to the field properties, what field postulates are gained by extending the natural numbers to the integers?

- -

ANSWER:

A_{id} and A_{in}.

- -

In extending the integers to the rational numbers what field postulate is gained?

- -

ANSWER:

M_{in}.

- -

It would seem, at first glance, that the system of rational numbers is quite sufficient for the development of more advanced mathematics since the system possesses all the field properties and is closed under the operations of addition, multiplication, subtraction, and division (except by zero). Such, however, is not the case. There is one very important property that the rational numbers lack, and which distinguishes this set from the reals. This is the property of ____.

ANSWER:

completeness.

Consider the following set of equations, and the questions that follow.

(a) $7x + 10 = 4x + 12$

(b) $3x^2 + 2 = x^2 + 6$

(c) $5x - 2 = 4x + 4$

(d) $4x + 21 = 15 + x$

(e) $x^2 + 4 = 3$

Which of the above equations have solutions in N?

Which have solutions in I?

Which have solutions in Q?

ANSWER:

(c);

(c) and (d);

(a), (c), and (d).

Does equation (b), which simplifies to $x^2 = 2$, have a solution in R?

ANSWER:

Yes; (A proof of this fact can be given, based on the Completeness Property of the real number system).

We will now prove that the equation $x^2 = 2$ has no solution in Q; i.e., there is no rational number a/b such that $(a/b)^2 = 2$. First, we need a definition and a lemma.

DEFINITION 10.3: A natural number n is a perfect square if and only if it is the square of a natural number; i.e., $n = p \cdot p$, where p is a natural number.

LEMMA 10.1: If n is a natural number, $n \neq 1$, then n is a perfect square if and only if each prime factor in its standard factorization occurs an even number of times.

PROOF: (a) Suppose n is a perfect square, $n \neq 1$. Show that each prime factor in its standard factorization occurs an even number of times.

- -

ANSWER:

Let $n = p \cdot p$, where p is a natural number. Let $p = 1 \cdot p_1 \cdot p_2 \cdots p_k$ be the standard factorization of p. Then $n = 1 \cdot p_1 \cdot p_1 \cdot p_2 \cdot p_2 \cdots p_k \cdot p_k$ is the (unique) standard factorization of n. Clearly each prime factor occurs an even number of times.

- -

(b) For the converse, show that if each prime factor in the standard factorization of n occurs an even number of times, then n is a perfect square.

- -

ANSWER:

Since each prime factor in the standard factorization of n occurs an even number of times, we may write

$n = 1 \cdot (p_1p_1)(p_2p_2)(p_3p_3) \cdots p_kp_k = (p_1p_2p_3 \cdots p_k)(p_1p_2p_3 \cdots p_k) = p \cdot p$, where $p = (p_1p_2p_3 \cdots p_k)$. Thus n is a perfect square by Definition 10.3.

THEOREM 10.1: There is no rational number a/b such that $(a/b)^2 = 2$. We may assume a and b to be positive integers, for if a were negative, then $-a$ is positive and we could consider $-a$ and b instead of a and b in the following proof.

PROOF: The proof will be by contradiction. We assume there *are* positive integers a and b such that $(a/b)^2 = 2$ and show this leads to a contradiction, hence the assumption is false.

(1) $(a/b)^2 = 2$.

Complete the proof, using Definition 10.3, Lemma 10.1, and the standard factorization theorem. You need not give reasons for the statements in your proof.

ANSWER:

a and b are positive integers (natural numbers) by assumption.

(1) $(a/b)^2 = 2$

(2) $a^2/b^2 = 2$

(3) $a^2 = 2b^2$

(4) $1 \cdot (a_1^2 \cdot a_2^2 \cdot a_3^2 \ldots) = 1 \cdot 2 \cdot (b_1^2 \cdot b_2^2 \cdot b_3^2 \ldots)$

where each of the expressions in parentheses represents the prime factorizations of a^2 and b^2 respectively, and each of the prime factors, a_i, b_i, occur an even number of times, by Definition 10.3 and Lemma 10.1. Both sides of equation (4) represent the standard factorization of the same number. But, the standard factorization of a number is unique, hence equation (4) cannot be true since 2 appears once, three times, or an *odd* number of times as a factor on the right, whereas it appears an *even* number of times, if at all, on the left side. Thus a contradiction has been reached, and the theorem is proved.

You should note that the above proof is valid if 2 is replaced by any prime natural number p. In fact, with a slight variation, it could be made to apply to any natural number that is not itself a perfect square; i.e., is not the square of a natural number.

REVIEW ITEMS

1. Reduce each of the following fractions of integers to lowest terms, if it is not already in lowest terms.

(a) 52/91

(b) -77/39

(c) 33/-95

ANSWER:

(a) 52/91 = 4/7;

(b) is in lowest terms;

(c) 33/-95 = -33/95 (To be in lowest terms, the denominator of a fraction must be positive.)

---

2. In which of the following subsets of Q is addition closed?

(a) Fractions of integers with denominator 2.

(b) Fractions of integers with numerator 3.

(c) Fractions of integers with denominator 2, 3, or 6.

ANSWER:

(a) and (c).

---

3. In which of the sets in Item 2 above is multiplication closed?

ANSWER:

None.

---

4. Recall the definition of a group in Unit II (Definition 2.3), and consider the set A of all rational numbers of the form a/2, where a is an integer.

(a) Does the set A form a group under the operation of addition? If not, what group postulates fail to hold?

ANSWER:

Yes, A forms a group under addition.

(b) Does the set A form a group under the operation of multiplication? If not, what group postulates fail to hold?

ANSWER:

No; Closure and M_{in}.

---

5. Which of the following two rational numbers is greater:
-13/27 or 24/-47 ?

ANSWER:

-13/27

---

6. What is true about the decimal representation of a rational number?

ANSWER:

The decimal either terminates or repeats a finite set of digits.

7. Convert the repeating decimal $3.2630\overline{630}$ to a fraction of integers in lowest terms.

ANSWER:

$\frac{1811}{555}$. This answer can be obtained as follows:

$$\begin{aligned}
\text{Let}\quad x &= 3.2630\overline{630} \\
x &= 3.2 + .0630\overline{630} \\
\text{Let}\quad y &= .0630\overline{630} \\
10y &= .630\overline{630} \\
10000y &= 630.\overline{630} = 630 + 10y \\
9990y &= 630 \\
y &= \frac{630}{9990} = \frac{7}{111} \\
\therefore\quad x &= 3 + 2/10 + \frac{7}{111} = \frac{3622}{1110} = \frac{1811}{555}
\end{aligned}$$

8. Show that the set of rational numbers between zero and one with numerator 1, i.e., the set $\{1/2, 1/3, 1/4, 1/5, \ldots\}$, is countable by defining a function that maps the natural numbers onto this set.

ANSWER:

$$\begin{array}{lcl}
1 & \xrightarrow{f} & 1/2 \\
2 & \longrightarrow & 1/3 \\
3 & \longrightarrow & 1/4 \\
\cdot & & \cdot \\
\cdot & & \cdot \\
\cdot & & \cdot
\end{array}$$

$$\begin{array}{ccc} n & \longrightarrow & 1/(n + 1) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \end{array}$$

Or, f is a function such that if n is a natural number, $n \xrightarrow{f} 1/(n + 1)$.

Which of the postulates for the real numbers is not valid for the system of rational numbers?

ANSWER:

The Completeness Postulate.

XI. COMPLEX NUMBERS

COMPLEX NUMBERS

DEFINITION AND BASIC OPERATIONS

Many high school text books introduce complex numbers by pointing out the lack of a solution, within the system of real numbers, of equations such as $x^2 + 1 = 0$. In order to remedy this situation a new symbol *i* is introduced, which, by definition, is to have the property that $i^2 = -1$. Then the expression $a + bi$, where a and b are real numbers, is called a complex number, *a* being the "real part" and *b* the "imaginary part". When this is done the complex number $a + bi$ is completely determined by the ordered pair (a, b) of real numbers a and b. Instead of following the above procedure we will *define* a complex number to be an ordered pair of real numbers. The definition of the symbol i is then very natural, whereas in the above described procedure it seems to be "pulled out of the air".

DEFINITION 11.1: A *complex number* is defined to be an ordered pair (x, y) of real numbers. x is called the *real part* and y is called the *imaginary part* of the complex number (x, y).

We will show that the set C of complex numbers, together with the operations of addition and multiplication which will presently be defined, is a field. We will also show that C contains a subsystem isomorphic to the real number field.

The complex numbers (x, y) and (z, w) are equal if and only if $x = z$ and $y = w$.

(1) (x, y) = (a, 0) if and only if x = ____ and y = ____.

(2) If 2 is the real part of a complex number and 5 is the imaginary part, then this complex number is written ____ in the ordered pair notation.

- -

ANSWER:

(1) a; 0.

(2) (2, 5)

- -

If (x, y) is a complex number then x is a real number. Is y a real number?

- -

ANSWER:

Yes. Even though y is called the imaginary part of the complex number (x, y) it is a real number.

- -

DEFINITION 11.2: The sum of the complex numbers (x, y) and (z, w) is the ordered pair (x + z, y + w).

This is written (x, y) + (z, w) = (x + z, y + w).

Does the definition for addition guarantee that C is closed under the operation of addition? Explain.

- -

ANSWER:

Yes. Since x, y, z and w are real numbers the sums x + z and y + w are real numbers. Therefore (x + z, y + w) is a complex number for any choice of x, y, z, and w.

- -

Since the definition of the operation of addition of complex numbers assigns the pair of complex numbers $[(x, y), (z, w)]$ to a unique complex number we may use function notation to exhibit this as follows:

$$[(x, y), (z, w)] \xrightarrow{+} (\_\_\_, \_\_\_).$$

ANSWER:

$(x + z, y + w)$.

State the commutative property of addition of complex numbers.

ANSWER:

If (x, y) and (z, w) are complex numbers, then

$(x, y) + (z, w) = (z, w) + (x, y)$.

Prove that the operation of addition of complex numbers has the commutative property.

ANSWER:

To show that the operation is commutative we must show that

$(x, y) + (z, w) = (z, w) + (x, y)$.

PROOF:

1.	$(x, y) + (z, w)$	$= (x + z, y + w)$	by Definition 11.2
2.	$(z, w) + (x, y)$	$= (z + x, w + y)$	by Definition 11.2
		$= (x + z, y + w)$	A_c for R
3.	$\therefore (x, y) + (z, w)$	$= (z, w) + (x, y)$	

Next we look for a complex number which is the identity element for addition in C.

(1) Complete the following:

(x, y) + (___, ___) = (x, y), for every complex number (x, y).

(2) Carry out the addition steps to show that you have selected the correct complex number.

- -

ANSWER:

(1) (0, 0)

(2) (x, y) + (0, 0) = (x + 0, y + 0) = (x, y).

- -

Also (0, 0) + (x, y) = (x, y). Therefore (0, 0) is the identity element for addition in C.

Is there an additive inverse for an element (x, y) of C? If there is, write the equation which defines it.

- -

ANSWER:

Yes; (x, y) + (-x, -y) = (0, 0) = (-x, -y) + (x, y).

- -

It can be shown (the proof is long, but not difficult) that the associative property for addition of complex numbers holds. State this property.

- -

ANSWER:

[(x, y) + (a, b)] + (c, d) = (x, y) + [(a, b) + (c, d)] for all (x, y), (a, b), (c, d) in C.

- -

Recall the definition of subtraction of real numbers: If a and b are real numbers, then the difference, b - a, is the unique real number d such that ____.

- -

ANSWER:

a + d = b.

- -

In the same manner, we define subtraction of complex numbers: If (x, y) and (z, w) are complex numbers, then the difference (z, w) - (x, y) is the unique complex number (r, s) such that ____.

- -

ANSWER:

(x, y) + (r, s) = (z, w).

- -

The difference (z, w) - (x, y) is given by (z, w) - (x, y) = (z - x, w - y). Find the value of (r, s) if (3, 1) = (r, s) + (5, -1).

- -

ANSWER:

(-2, 2)

- -

DEFINITION 11.3: The product of the complex numbers (x, y) and (z, w) is the complex number (xz - yw, xw + yz); this is written (x, y) · (z, w) = (xz - yw, xw + yz).

This definition guarantees closure, commutativity and associativity for the operation of multiplication. (You should be able to prove that these properties hold, using proofs similar to those for addition.)

Apply the definition of multiplication of complex numbers to find the product $(x, y) \cdot (1, 0)$.

- -

ANSWER:

(x, y). Solution $(x, y) \cdot (1, 0) = (x \cdot 1 - y \cdot 0,\ x \cdot 0 + y \cdot 1) = (x, y)$.

- -

The answer to the previous problem suggests a special name for the complex number $(1, 0)$. What is it?

State (in full) the property for complex numbers associated with this element.

- -

ANSWER:

Identity element for multiplication.

The complex number $(1, 0)$ is the identity element for multiplication of complex numbers; i.e., $(x, y) \cdot (1, 0) = (1, 0) \cdot (x, y) = (x, y)$ for all elements (x, y) of C.

- -

Find the product $(x, y) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$. Assume $(x, y) \neq (0, 0)$.

- -

ANSWER:

$(1, 0)$. Solution: $(x, y) \cdot \left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right) = \left(\frac{x^2}{x^2 + y^2} - \frac{-y^2}{x^2 + y^2}, \frac{-xy}{x^2 + y^2} + \frac{xy}{x^2 + y^2}\right) = (1, 0)$.

- -

$\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right)$ is called the ____ of (x, y).

- -

ANSWER:

multiplicative inverse

- -

Show that $(4/25, -3/25)$ is the multiplicative inverse of $(4, 3)$.

- -

ANSWER:

Two solutions are shown below.

Solution (1): $(4, 3) \cdot (4/25, -3/25) = \left(\frac{16 + 9}{25}, \frac{12 - 12}{25}\right) = (1, 0)$.

Solution (2): If $(x, y) = (4, 3)$ then $\left(\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}\right) = \left(\frac{4}{16 + 9}, \frac{-3}{16 + 9}\right) = (4/25, -3/25)$.

- -

Division for real numbers has been defined in terms of multiplication. By analogy, for complex numbers, if $(c, d) \neq (0, 0)$, then $(a, b) \div (c, d) = (x, y)$ if and only if $(c, d) \cdot (x, y) = (a, b)$. The problem then is to find values for x and y which satisfy the equation $(c, d) \cdot (x, y) = (a, b)$.

First find the product $(c, d) \cdot (x, y)$.

- -

ANSWER:

$(cx - dy, cy + dx)$

- -

Now, by the definition of equality of complex numbers we know that $(cx - dy, cy + dx) = (a, b)$ if and only if $cx - dy = $ _____.

$cy + dx = $ _____.

- -

ANSWER:

a.

b.

- -

Solve the system of equations below for x and y.

$cx - dy = a$

$cy + dx = b$

- -

ANSWER:

$x = \frac{ac + bd}{c^2 + d^2}, \quad y = \frac{bc - ad}{c^2 + d^2}$

- -

Note that this system of equations has a solution provided $c^2 + d^2 \neq 0$. List all values for c and d such that $c^2 + d^2 = 0$.

- -

ANSWER:

$c^2 + d^2 = 0$ if and only if $c = 0$ and $d = 0$.

- -

Hence, if we make the restriction that $(c, d) \neq (0, 0)$, then (x, y) exists and division of complex numbers is defined.

$(a, b) \div (c, d) = \left(\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2}\right)$

(1) Find the quotient $(3, 4) \div (2, 1)$.

(2) Check your work by multiplication, i.e., if $(3, 4) \div (2, 1) = (x, y)$ then $(2, 1) \cdot (x, y) = (3, 4)$.

- -

ANSWER:

(1) $(2, 1)$.

(2) $(2, 1) \cdot (2, 1) = (4 - 1, 2 + 2) = (3, 4)$.

- -

Apply the definition of division to find the multiplicative inverse of the complex number $(2, -5)$, i.e., if $(2, -5) \cdot (x, y) = (1, 0)$, then $(x, y) =$ ____.

ANSWER:

$(x, y) = (1, 0) \div (2, -5) = (2/29, 5/29)$.

Find by the method suggested above the multiplicative inverse of the complex number (a, b) where $(a, b) \neq (0, 0)$.

ANSWER:

$(a, b)(x, y) = (1, 0)$

$(x, y) = (1, 0) \div (a, b) = \left(\frac{1 \cdot a + 0 \cdot b}{a^2 + b^2}, \frac{0 \cdot a - 1 \cdot b}{a^2 + b^2}\right) =$
$\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$

Note that this answer agrees with that found previously.

Write a complete proof to show that in the system C the distributive property holds, i.e., if (a, b), (c, d), (e, f) are any complex numbers, then $(a, b) \cdot [(c, d) + (e, f)] = (a, b)(c, d) + (a, b)(e, f)$. (You need not list all field properties of the real numbers that are used. However, point out where Property D for real numbers is used.)

ANSWER:

Step (1) Left member:

$$\begin{aligned}(a, b) \cdot [(c, d) + (e, f)] &= (a, b) \cdot [(c + e, d + f)]\\ &= [a(c + e) - b(d + f),\\ &\quad a(d + f) + b(c + e)]\end{aligned}$$

$$= [ac + ae - bd - bf,\ ad + af + bc + be]$$

Property D

Step (2) Right member:

$$\begin{aligned}(a, b) \cdot (c, d) + (a, b) \cdot (e, f) &= (ac - bd,\ bc + ad) + (ae - bf,\ be + af)\\ &= [(ac - bd) + (ae - bf),\ (bc + ad) + (be + af)]\\ &= [ac + ae - bd - bf,\ ad + af + bc + be]\end{aligned}$$

Step (3) Hence:

$$(a, b) \cdot [(c, d) + (e, f)] = (a, b) \cdot (c, d) + (a, b) \cdot (e, f).$$

- -

Let us review the properties the system C has been shown to possess. There is a set C of elements (called complex numbers). There are two closed operations called "addition" and "multiplication" which are defined on C so that the following properties hold:

(1) Commutative properties for addition and multiplication.

(2) Associative properties for addition and multiplication.

(3) Distributive property for multiplication over addition.

(4) There is an element (____, ____) such that (x, y) + (____, ____) = (____, ____) + (x, y) = (x, y) for every element (x, y) of C. (The identity element for addition.)

(5) There is an element (____, ____) such that (x, y) · (____, ____) = (____, ____) · (x, y) = (x, y) for every element (x, y) of C. (The identity element for multiplication.)

(6) For each (x, y) of C there exists an inverse element, (____, ____), for addition such that (x, y) + (____, ____) = (____, ____).

(7) For each (x, y) of C, (x, y) ≠ (0, 0), there exists an inverse element, (____, ____), for multiplication such that (x, y) · (____, ____) = (____, ____).

(8) Since C has the above properties, it is a _____.

ANSWER:

(4) $(0, 0)$ $\quad (x, y) + (0, 0) = (0, 0) + (x, y) = (x, y)$

(5) $(1, 0)$ $\quad (x, y) \cdot (1, 0) = (1, 0) \cdot (x, y) = (x, y)$

(6) $(-x, -y)$ $\quad (x, y) + (-x, -y) = (0, 0)$

(7) $\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}$ $\quad (x, y) \cdot (\frac{x}{x^2 + y^2}, \frac{-y}{x^2 + y^2}) = (1, 0)$

(8) field

We have shown that the system of complex numbers is a field. Therefore all the properties which were developed in Unit II on the basis of the field postulates are properties of the system of complex numbers as well as the system of real numbers.

ISOMORPHISM OF A SUBSYSTEM OF C WITH THE SYSTEM OF REAL NUMBERS

Our next aim is to find a subsystem C' of C which is isomorphic to R (the system of real numbers). An isomorphism from a subsystem C' onto R is a one-to-one correspondence (or reversible function) from C' onto R which preserves the operations of addition and multiplication.

The additive identity for the complex numbers is $(0, 0)$. This suggests that in the desired isomorphism the complex number $(0, 0)$ should correspond to the real number ____, because ____.

ANSWER:

0, because 0 is the additive identity for R.

The multiplicative identity for the complex numbers is _____. This suggest that the complex number ____ should correspond to the real number ____.

- -

ANSWER:

(1, 0).

(1, 0); 1.

- -

We can continue the correspondence of elements suggested by the previous item and display it as a function ϕ which assigns each complex number of the form (a, 0) to the unique real number a, as shown below.

(0, 0) $\xrightarrow{\phi}$ 0
(1, 0) $\xrightarrow{\phi}$ 1
(2, 0) $\xrightarrow{\phi}$ ___
(-3, 0) $\xrightarrow{\phi}$ ___
($\sqrt{5}$, 0) $\xrightarrow{\phi}$ ___
(7/9, 0) $\xrightarrow{\phi}$ ___
. .
. .
. .
(x, 0) $\xrightarrow{\phi}$ ___
. .
. .
. .

- -

ANSWER:

2
-3
$\sqrt{5}$
7/9

x

---

(1) What is the domain of ϕ?

(2) What is the range of ϕ?

ANSWER:

(1) The set of all complex numbers of the form $(a, 0)$.

(2) The set of all real numbers.

To show that ϕ is a reversible function we must show that each element of the range of ϕ is paired with ____.

ANSWER:

exactly one element of the domain of ϕ.

Prove that ϕ is a reversible function.

ANSWER:

PROOF: Suppose $(x, 0) \xrightarrow{\phi} a$ and $(y, 0) \xrightarrow{\phi} a$, we must show that $x = y$.

By definition of ϕ,

$$\begin{aligned} (x, 0) &\xrightarrow{\phi} a \text{ implies } x = a \\ (y, 0) &\xrightarrow{\phi} a \text{ implies } y = a \\ &\therefore x = y \end{aligned}$$

Thus we have shown that ϕ is a reversible function from C' onto R (there is a one-to-one correspondence between the elements of C' and R.)

Show that the correspondence preserves sums:

$$\begin{tikzcd}(a, 0) \arrow[d] & + & (b, 0) \arrow[d] & = & \_\_\_\_ \arrow[d] \\ a & + & b & = & \_\_\_\_\end{tikzcd}$$

- -

ANSWER:

If we add, $(a, 0) + (b, 0) = (a + b, 0)$, we get a result which corresponds to the real number $a + b$. This is the result we get when we add the real numbers a and b.

$$\begin{tikzcd}(a, 0) \arrow[d] & + & (b, 0) \arrow[d] & = & (a + b, 0) \arrow[d] \\ a & + & b & = & a + b\end{tikzcd}$$

- -

Show that the correspondence preserves products.

- -

ANSWER:

When we multiply, $(a, 0) \cdot (b, 0) = (ab - 0, 0 \cdot b + a \cdot 0) = (ab, 0)$. The complex number $(ab, 0)$ corresponds to the real number ab which is the product of the real numbers which correspond to $(a, 0)$ and $(b, 0)$.

$$\begin{tikzcd}(a, 0) \arrow[d] & \cdot & (b, 0) \arrow[d] & = & (ab, 0) \arrow[d] \\ a & \cdot & b & = & ab\end{tikzcd}$$

- -

The work of the preceding items shows that we can establish a correspondence between the elements of the subset C' of the complex numbers and the set of all real numbers which is "one-to-one" and "onto". This correspondence preserves sums and products. Thus we know that the subsystem C' of C is ____ to the systems of all real numbers.

- -

ANSWER:
isomorphic

- -

Strictly speaking, the set of complex numbers as we have defined it does not contain the real numbers. However, we have shown that the system of complex numbers has a subsystem which is isomorphic to the system of real numbers under the correspondence $(a, 0) \longrightarrow a$, for each real number a.

It is customary to identify the ordered pair $(a, 0)$ with the real number a, and it is in this sense that the reals are contained in the set of complex numbers. You are familiar with this idea of identification in analytic geometry. In graphing on a coordinate plane each point in the plane is associated with an ordered pair of real numbers (which give the coordinates of the point). However, it is common to designate points on the horizontal axis by real numbers instead of ordered pairs. When we do this we are identifying the ordered pair $(a, 0)$ with the real number a. This convention of graphing makes it very natural to associate complex numbers with points in the plane; and in this association real numbers correspond to points on the abscissa (horizontal axis).

Let w be the complex number $(0, 1)$. Show that $(0, 1)$ is a solution to the equation $w^2 = (-1, 0)$. [Here, w denotes a complex number, i.e., an ordered pair of real numbers.]

- -

ANSWER:
$(0, 1)^2 = (0, 1) \cdot (0, 1) = (0 - 1, 0 + 0) = (-1, 0)$.

- -

Are there any other solutions to the equation $w^2 = (-1, 0)$ in the set of complex numbers? (Recall that in the real number system the equation $w^2 = 1$ has two solutions, $w = 1$ and $w = -1$.)

- -

ANSWER:

Yes, $(0, -1)$ is also a solution, since $(0, -1)^2 = (0, -1)(0, -1) = (0 - 1, 0 + 0) = (-1, 0)$.

- -

In the last two items we have shown that in the complex number system if $w = w_1 = (0, 1)$ or $w = w_2 = (0, -1)$ then $w^2 = (-1, 0)$.

Here w^2 corresponds to the real number ____.

Does w_1 or w_2 correspond to any real number?

- -

ANSWER:

w^2 corresponds to -1 but there is no real number corresponding to either w_1 or w_2.

- -

We are ready now to relate the (a, b) notation to the more familiar $a + bi$ notation for complex numbers. First you should observe that

$(a, 0) + (0, b) =$ ____

$(b, 0) \cdot (0, 1) =$ ____

- -

ANSWER:

(a, b)

$(0, b)$

- -

In the notation a + bi, a and b are real numbers and i is the complex number (0, 1). Rewrite a + bi, replacing a, b, and i each by ordered pairs. (Refer to the isomorphism which has been established between R and C'.) Simplify the result using the properties of complex numbers.

a + bi =

- -

ANSWER:

$$\begin{aligned} a + bi &= (a, 0) + (b, 0)(0, 1) \\ &= (a, 0) + (0, b) \\ &= (a, b) \end{aligned}$$

- -

Write (a + c, b + d) in a + bi notation.

- -

ANSWER:

(a + c) + (b + d)i

- -

We wish to emphasize that the notation a + bi for the complex number (a, b) is a shorthand way of writing

$(a, 0) + (b, 0) \cdot (0, 1)$.

The complex numbers (a, 0) and (b, 0) are replaced by the corresponding real numbers a and b and (0, 1) is replaced by the letter i.

Simplify $(2, 0) + (3, 0) \cdot (0, 1)$ to a single ordered pair using the definition of addition and multiplication in C. Show each step.

- -

ANSWER:

$$(2, 0) + (3, 0) \cdot (0, 1) = (2, 0) + (3 \cdot 0 - 0 \cdot 1, 3 \cdot 1 + 0 \cdot 0)$$

$$= (2, 0) + (0, 3)$$
$$= (2 + 0, 0 + 3)$$
$$= (2, 3)$$

- -

So we have

$2 + 3i = (2, 0) + (3, 0) \cdot (0, 1) = (2, 3)$.

Write $c + 2i$ in ordered pair notation.

- -

ANSWER:

$(c, 2)$. Be careful to avoid writing $(2, 2i)$.

- -

Write $(6, -2)$ in $a + bi$ notation.

- -

ANSWER:

$6 + (-2)i$ or $6 - 2i$

- -

If $i = (0, 1)$ then $i^2 = (0, 1)^2 = (\_\_\_, \_\_\_)$.

Rewrite your answer in the $a + bi$ notation.

- -

ANSWER:

$(-1, 0)$

$-1 + 0i$ or -1

- -

Addition in the $a + bi$ notation agrees with addition in the (a, b) notation.

In (a, b) notation $(a, b) + (c, d) = (a + c, b + d)$.

In $a + bi$ notation $(a + bi) + (c + di) =$ ____.

ANSWER:

$(a + c) + (b + d)i$

Find the sums

(1) $(4 + 3i) + (2 + 8i) =$ ____.

(2) $(4, 3) + (2, 8) =$ ____.

(3) $(3 + 2i) + (-3 - 2i) =$ ____.

(4) $(3, 2) + (-3, -2) =$ ____.

ANSWER:

(1) $6 + 11i$

(2) $(6, 11)$ (Again we emphasize, do not write $(6, 11i)$.)

(3) $0 + 0i = 0$

(4) $(0, 0)$

Multiplication in the $a + bi$ notation agrees with multiplication in the (a, b) notation.

In ordered pair notation $(a, b) \cdot (c, d) =$ _____.

In $a + bi$ notation $(a + bi) \cdot (c + di) =$ _____.

ANSWER:

$(ac - bd, bc + ad)$

$(ac - bd) + (bc + ad)i$

Find the product of $(a + bi) \cdot (c + di)$ by applying the associative, commutative, and distributive laws and replacing i^2 by -1. (Reasons for steps are not required.) This answer should agree with the definition shown above for the same product.

- -

ANSWER:

$$\begin{aligned}(a + bi)(c + di) &= (a + bi)c + (a + bi)di \\ &= ac + bci + adi + bdi^2 \\ &= ac + (bc + ad)i + bd(-1) \\ &= (ac - bd) + (bc + ad)i\end{aligned}$$

- -

Find the products:

(1) $(1 + i) \cdot (1 - i) =$ _____.

(2) $(5 + 3i) \cdot (5/34 - 3/34\ i) =$ ____.

- -

ANSWER:

(1) $2 + 0i = 2$

(2) $1 + 0i = 1$

- -

Some of the terminology used with complex numbers is rather unfortunate. In the complex number $c = a + bi$, the real number $\underline{a}$ is called the real part of C, and the real number $\underline{b}$ is called the imaginary part of C. There is a historical reason behind this choice of words that goes back to the days when complex numbers were considered in some sense not as "real" as real numbers. It would perhaps be better to identify these numbers as the first and second components respectively, (or merely as the "non i" part and the "i" part) of the complex number, but the other terminology still continues to be most frequently used.

If $a = 0$ and $b \neq 0$, then the complex number $a + bi$ is written simply as $\underline{bi}$ and is called a pure imaginary number. If $b = 0$ then the complex number $a + bi$ is written simply as a and is a real number.

453

CONJUGATE OF A COMPLEX NUMBER

DEFINITION 11.4: If $c = a + bi$ is a complex number, then the conjugate of c is the complex number $\overline{c} = a + (-b)i = a - bi$. We shall use the notation $\overline{c} = \overline{a + bi} = a - bi$.

According to this definition write each of the following:

$\overline{c} = \overline{3 + 4i} =$ ____.

$\overline{c} = \overline{2 - 6i} =$ ____.

$\overline{c} = \overline{i} =$ ____.

$\overline{c} = \overline{2} =$ ____.

ANSWER:

$3 - 4i$

$2 + 6i$

$-i$

2

Several important properties relating a complex number to its conjugate are given in the following theorems:

THEOREM 11.1: If c is a complex number, then $c \cdot \overline{c}$ is a real number. If $c \neq 0$ then $c \cdot \overline{c} > 0$.

THEOREM 11.2: If c is a complex number then $\overline{\overline{c}} = c$. (The conjugate of the conjugate of c is c.)

THEOREM 11.3: If c and d are complex numbers, then $\overline{c} + \overline{d} = \overline{c + d}$.

THEOREM 11.4: If c and d are complex numbers, then $\overline{c} \cdot \overline{d} = \overline{c \cdot d}$.

THEOREM 11.5: If c is a complex number, then $(\overline{c})^n = \overline{c^n}$, for each natural number n.

The proofs for the above theorems depend on definitions and preceding theorems. For example, to prove Theorem 11.4, let $c = a + bi$ and $d = x + yi$, then apply the definition of conjugate of a complex number and the definition of multiplication. Write the proof (supply reasons for the steps which depend on definitions or theorems on complex numbers).

- -

ANSWER:

PROOF:

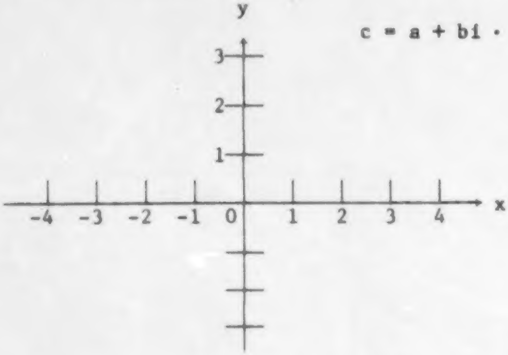
	Statement	Reason
1.	If $c = a + bi$ and $d = x + yi$	
	then $\overline{c} = a - bi$ and $\overline{d} = x - yi$	Definition of conjugate
2.	$\overline{c} \cdot \overline{d} = (a - bi)(x - yi)$	
	$= (ax - by) - (bx + ay)i$	Definition of multiplication
3.	$c \cdot d = (a + bi)(x + yi)$	
	$= (ax - by) + (bx + ay)i$	Definition of multiplication
4.	$\overline{c \cdot d} = (ax - by) - (bx + ay)i$	Definition of conjugate
5.	$\therefore \overline{c} \cdot \overline{d} = \overline{c \cdot d}$	

- -

GRAPHING AND ABSOLUTE VALUE

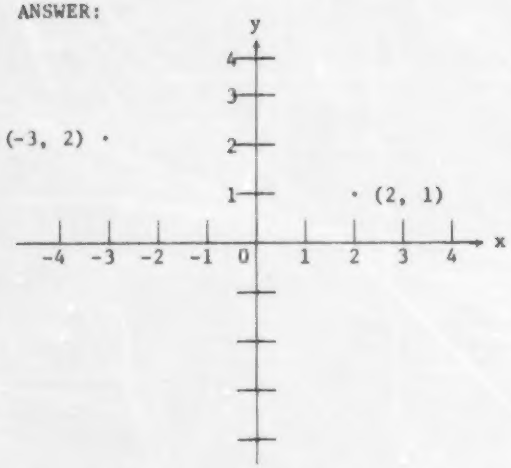
In earlier units you have studied the geometrical representation of real numbers as points on a line. Since a complex number is defined as an ordered pair of real numbers, and since we are familiar with the association of pairs of real numbers with points in a plane, it is natural to represent complex numbers as points in a plane. We therefore associate with each complex number $c = a + bi = (a, b)$, where a and b are real numbers, the point (a, b) in a coordinate plane. (See sketch on next page.)

On the same coordinate plane locate and label the points corresponding to the complex numbers 2 + i and -3 + 2i.


y
3
2
1
-4
-3
-2
-1
0
1
2
3
4
x

c = a + bi · (a, b)

ANSWER:


y
4
3
2
1
(-3, 2)
(2, 1)
-4
-3
-2
-1
0
1
2
3
4
x

Where are the points which correspond to complex numbers of the form a + 0i? ____; of the form 0 + bi? _____.

ANSWER:

on the x axis;

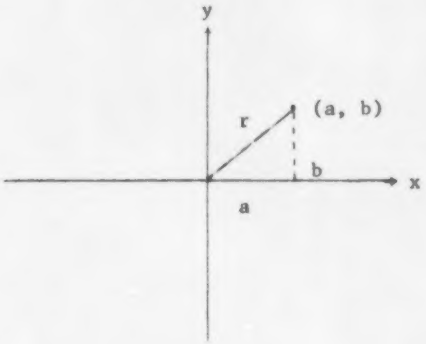
on the y axis.

- -

If we let r denote the distance from the origin to the point (a, b), representing the complex number $c = a + bi$, then

$$r^2 = a^2 + b^2$$
$$r = \sqrt{a^2 + b^2}$$

We speak of this distance r as the absolute value of c; hence we have the following definition for the absolute value of a complex number.



DEFINITION 11.5: If c is the complex number $a + bi$ then $|c| = \sqrt{a^2 + b^2}$.

Thus if $c = 3 + 4i$ then $|c| =$ ____. Note that $|c|$ is a non-negative real number.

- -

ANSWER:

$\sqrt{9 + 16} = \sqrt{25} = 5$

- -

Where in the coordinate plane are the points which correspond to the complex numbers which have absolute value 1?

ANSWER:

On the circle with center at (0, 0) and radius 1 (the unit circle).

If the absolute value of a complex number c is greater than 1, i.e., $|c| > 1$, what is the location on the coordinate plane of the point c?

ANSWER:

c lies outside the unit circle.

THEOREM 11.6: $c \cdot \overline{c} = |c|^2$, for each complex number c.

Write a proof giving reasons for steps which depend on definitions or theorems relating to complex numbers.

ANSWER:

1. Let $c = a + bi$, then $\overline{c} = a - bi$
2. $c \cdot \overline{c} = (a + bi)(a - bi) = a^2 + b^2 + 0i = a^2 + b^2$
3. Since $a^2 + b^2 = (\sqrt{a^2 + b^2})^2$

then $c \cdot \overline{c} = (\sqrt{a^2 + b^2})^2 = |c|^2$

1. Definition of conjugate
2. Definition of multiplication
3. Definition of absolute value

The result of the preceding item is useful in computing the multiplicative inverse of a complex number and in computing quotients of complex numbers.

(1) Recall that in ordered pair notation the multiplicative inverse of (a, b) is ____.

(2) In $a + bi$ notation the multiplicative inverse of the complex number $a + bi$ is ____.

- -

ANSWER:

(1) $\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$

(2) $\frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i$

- -

Let $c = a + bi$. Show that $\frac{1}{|c|^2} \cdot \overline{c}$ is the multiplicative inverse of c. Assume $c \neq 0$. (Reasons may be omitted.)

- -

ANSWER:

$$\begin{aligned} \frac{1}{|c|^2}(\overline{c}) &= \left(\frac{1}{\sqrt{a^2 + b^2}}\right)^2 (a - bi) \\ &= \frac{1}{a^2 + b^2}(a - bi) \\ &= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \end{aligned}$$

- -

Apply the preceding formula to find the multiplicative inverse of $2 + 3i$.

- -

ANSWER:

$$\frac{1}{|c|^2} \cdot \overline{c} = \left(\frac{1}{\sqrt{4 + 9}}\right)^2 \cdot (2 - 3i) = 1/13(2 - 3i) = \frac{2}{13} + \frac{-3}{13}\, i$$

Theorem 11.6 is applied as follows to find the quotient c/d.

$c/d = c/d \cdot \overline{d}/\overline{d} = c\overline{d}/|d|^2$

Find the quotient $\frac{1 + i}{2 - i}$. Write the answer in the form $x + yi$.

ANSWER:

$$\frac{1 + i}{2 - i} = \frac{1 + i}{2 - i} \cdot \frac{2 + i}{2 + i} = \frac{(1 + i)(2 + i)}{(2 - i)(2 + i)} = \frac{1 + 3i}{5} = \frac{1}{5} + \frac{3i}{5}$$

A proof of the following theorem can be made without changing the complex numbers to the $a + bi$ form. Write your proof supplying reasons which are based on theorems or definitions for complex numbers.

THEOREM 11.7: If c and d are complex numbers, $d \neq 0$, then $\overline{(c/d)} = \overline{c}/\overline{d}$. [Hint: Show that $1/\overline{d} = \overline{1}/d$, and apply Theorem 11.4.]

If you feel that you have given a complete proof of Theorem 11.7, go to the $\boxed{\dagger\dagger}$ on page 443. If not, go to the next item, below.

$\overline{1}/d = \overline{1/|d|^2 \cdot \overline{d}}$

$= \overline{1/|d|^2} \cdot \overline{\overline{d}}$ Theorem 11.4

$= 1/|d|^2 \cdot d$ Theorem 11.2

$$= d/|d|^2$$

Why does $\overline{1/|d|^2} = 1/|d|^2$?

ANSWER:

$1/|d|^2$ is a real number.

Go back to your proof of Theorem 11.7. Make additions or corrections. If you have not already done so, show as above that $1/\overline{d} = d/|d|^2$, then complete the proof.

$\boxed{\dagger\dagger}$ ANSWER:

PROOF:

$$1/\overline{d} = 1/\overline{d} \cdot d/d$$

$$= \frac{1 \cdot d}{\overline{d} \cdot d} = d/|d|^2 \qquad \text{Theorem 11.6}$$

$$\overline{1/d} = \overline{1/|d|^2 \cdot \overline{d}}$$

$$= \overline{1/|d|^2} \cdot \overline{\overline{d}} \qquad \text{Theorem 11.4}$$

$$= 1/|d|^2 \cdot d \qquad \text{Theorem 11.2}$$

$$= d/|d|^2$$

Therefore

$$\overline{1/d} = 1/\overline{d}$$

Then

$$\overline{c/d} = \overline{c \cdot 1/d}$$

$$= \overline{c} \cdot \overline{1/d} \qquad \text{Theorem 11.4}$$

$= \bar{c} \cdot 1/\bar{d}$ By the first part of proof

$= \bar{c}/\bar{d}$

Show that $|c \cdot d|^2 = |c|^2 \cdot |d|^2$. You may omit reasons, but refer to your list of theorems as often as necessary for suggestions.

ANSWER:

$$|cd|^2 = cd \cdot \overline{cd} = cd \cdot \bar{c} \cdot \bar{d} = c \cdot \bar{c} \cdot d \cdot \bar{d} = |c|^2 \cdot |d|^2.$$

From the equation $|c \cdot d|^2 = |c|^2 \cdot |d|^2$, we obtain easily the following theorem:

THEOREM 11.8: If c and d are complex numbers, then $|c \cdot d| = |c| \cdot |d|$. A theorem related to Theorem 11.8 is the following:

THEOREM 11.9: If c and d are complex numbers, $d \neq 0$, then $|c/d| = |c|/|d|$.

To prove Theorem 11.9, it is sufficient to show that $|c/d|^2 = |c|^2/|d|^2$. Prove that this is true. List as reasons any theorems from this unit which are used.

ANSWER:

$|c/d|^2 = c/d \cdot \overline{c/d}$ Theorem 11.6

$= c/d \cdot \bar{c}/\bar{d}$ Theorem 11.7

$= \dfrac{c \cdot \bar{c}}{d \cdot \bar{d}}$

$= |c|^2/|d|^2$ Theorem 11.6

Hence $|c/d| = |c|/|d|$

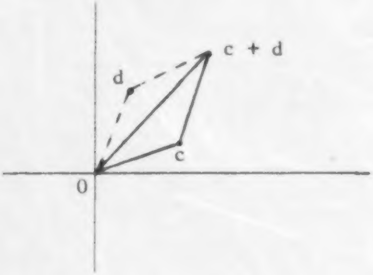
- -

In Unit VI, Theorem 6.4, we showed that if c and d are real numbers then $|c + d| \leq |c| + |d|$, the so-called "triangle inequality". This inequality is also valid if c and d are complex numbers.

THEOREM 11.10: If c and d are complex numbers, then $|c + d| \leq |c| + |d|$.

We will not give a proof of this theorem here.

If c and d are complex numbers and if 0, c, and d do not all lie on a line in the plane, then addition of c and d can be accomplished by the so-called "parallelogram rule". The points 0, c, d and $c + d$ are vertices of a parallelogram. This is illustrated in the accompanying graph.



The length of the segment from 0 to c is $|c|$.

The length of the segment from 0 to $(c + d)$ is ____.

The length of the segment from c to $(c + d)$ is ____.

- -

ANSWER:

$|c + d|$.

$|d|$.

- -

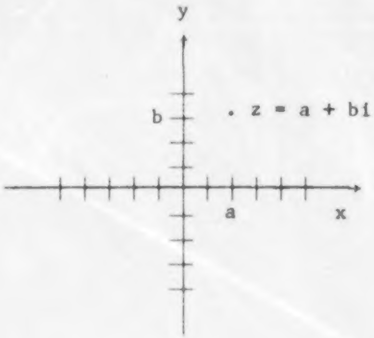
State a geometric property of triangles which tells us that $|c + d| < |c| + |d|$.

- -

ANSWER:
The length of one side of a triangle is less than the sum of the lengths of the other two sides.

- -

The remainder of this unit consists of algebraic and geometric applications relating to complex numbers.



Let $z = a + bi$ be the point indicated on the graph.

(1) Locate the point $\bar{z}$, the point $-\bar{z}$, and the point $-z$.

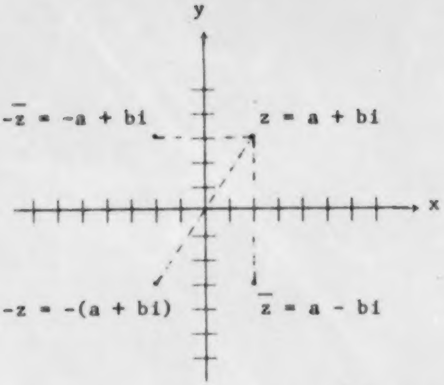
(2) Note that $\bar{z}$ is the reflection of z across the ____ axis, that $-\bar{z}$ is the reflection of z across the ____ axis, that $-z$ is the reflection of z ____.

- -

ANSWER:

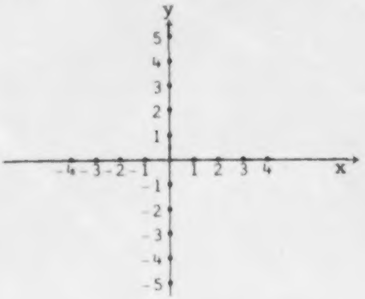
(1) See graph on next page.

(2) x (or real)
y (or imaginary)
through (across) the origin


y
$-\bar{z} = -a + bi$
$z = a + bi$
x
$-z = -(a + bi)$
$\bar{z} = a - bi$

- -

Show graphically the set of complex numbers z which satisfy the equation $z = 1/z$.


y
5
4
3
2
1
-4
-3
-2
-1
1
2
3
4
x
-1
-2
-3
-4
-5

- -

ANSWER:

$z \neq 0$

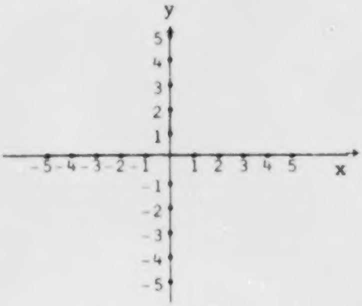
$$z = 1/z \quad — \quad z^2 = 1 \iff z^2 - 1 = 0$$

$$\iff (z - 1)(z + 1) = 0$$

$$\iff z = +1 \text{ or } z = -1$$

The solution set is $\{1, -1\}$.

Show graphically the set of complex numbers z which satisfy the equation $\overline{z} = 1/z$.


y
5
4
3
2
1
-5 -4 -3 -2 -1
1 2 3 4 5
x
-1
-2
-3
-4
-5

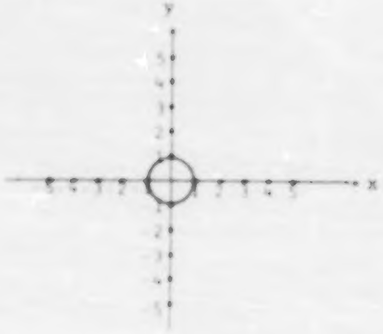
ANSWER:

$z \neq 0$

$\overline{z} = 1/z \iff \overline{z} \cdot z = 1 \iff |z|^2 = 1$

If $z = a + bi$ then $|z|^2 = a^2 + b^2 = 1$.

Hence z may be any point on the unit circle.


y
5
4
3
2
1
-5
-4
-3
-2
1
2
3
4
5
x
-1
-2
-3
-4
-5

Show graphically the set of complex numbers z which satisfy the equation $z + \overline{z} = 3$.

y
5
4
3
2
1
-4
-3
-2
-1
1
2
3
4
x
-1
-2
-3
-4
-5

ANSWER:

Let $z = a + bi$, $\overline{z} = a - bi$

then $z + \overline{z} = 3 \iff 2a = 3 \iff a = 3/2$

y
x
3
2
1
-1
-2
-3
-4
-3
-2
-1
1
2
3
4

- -

Let $c_1 = x_1 + y_1 i$ and $c_2 = x_2 + y_2 i$; find $|c_2 - c_1|$.

- -

ANSWER:

$$c_2 - c_1 = (x_2 - x_1) + (y_2 - y_1)i$$

$$|c_2 - c_1| = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

- -

To give a geometric interpretation to the previous problem we recall that $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ represents the distance between the two points (x_1, y_1) and (x_2, y_2) on a coordinate plane, hence $|c_2 - c_1|$ represents ___.

- -

ANSWER:

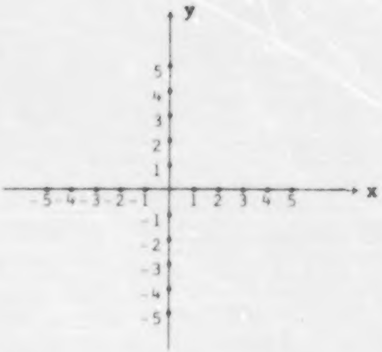
the distance between the points c_1 and c_2.

- -

Let $c_1 = -3 + 4i$ and $c_2 = -5 - 4i$.

(1) Locate the points corresponding to these numbers on a coordinate plane.

(2) Find $|c_2 - c_1|$


y
x
5
4
3
2
1
-1
-2
-3
-4
-5
-5 -4 -3 -2 -1
1 2 3 4 5

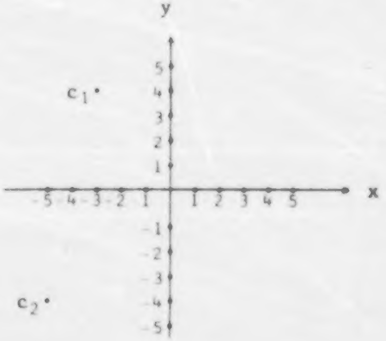
- -

ANSWER:

(1) See the graph.

(2) $|c_2 - c_1| = \sqrt{(-5 + 3)^2 + (-4 - 4)^2}$

$= \sqrt{68}$ or $2\sqrt{17}$


y
x
c_1
c_2
5
4
3
2
1
-1
-2
-3
-4
-5
-5 -4 -3 -2 -1
1 2 3 4 5

- -

$|c_2 - c_1|$ represents the distance from the complex number c_2 to the complex number c_1. If the distance from a complex number z to the complex number 2 is 3, then z is a point on the circle with center at ____ and radius ____.

- -

ANSWER:

(2, 0)

3.

Thus the complex numbers z satisfying the equation $|z - 2| = 3$ are those on the circle with center (2, 0) and radius 3.

Find the set of complex numbers z which satisfy the condition $|z + 2| > 3$.

ANSWER:

The set of complex numbers exterior to the circle with center (-2, 0) and radius 3.

Note: $|z + 2| = |z - (-2)|$. The distance from z to -2 is greater than 3.

Find the set of complex numbers z which satisfy the condition $|z - 3i| < 4$.

ANSWER:

The set of complex numbers interior to the circle with center at (0, 3) and radius 4.

Find the set of complex numbers z which satisfy the condition $|z - z_0| \leq r$, $r > 0$, where z_0 is a complex number.

ANSWER:

The set of complex numbers interior to or on the circle with center at z_0 and radius r.

Give a geometric interpretation of the inequality $|z_1| < |z_2|$.

ANSWER:

The distance from z_1 to the origin is less than the distance from z_2 to the origin.

To solve the inequality $\left|\frac{z-1}{z+1}\right| < 1$ we start with the statement

$$\begin{aligned} \left|\frac{z-1}{z+1}\right| < 1 &\Leftrightarrow z \neq -1 \text{ and } |z-1| < |z+1| \\ &\Leftrightarrow z \neq -1 \text{ and } |z-1| < |z-(-1)| \end{aligned}$$

What information does this statement give you about the location of z?

ANSWER:

z is nearer the point 1 than the point -1;

or z is in the right half plane (to the right of the y-axis);

or the real part of z is positive.

Note: The solution to $\left|\frac{z-1}{z+1}\right| < 1$ can be displayed as follows:

$$\begin{aligned} \left|\frac{z-1}{z+1}\right| < 1 &\Leftrightarrow z \neq -1 \text{ and } |z-1| < |z-(-1)| \\ &\Leftrightarrow z \text{ is nearer the point 1 than the point } -1 \\ &\Leftrightarrow z \text{ is in the right half plane} \\ &\Leftrightarrow \text{Real part of } z > 0. \end{aligned}$$

If a function f is defined by $f(z) = \frac{z-1}{z+1}$, $z \neq -1$ then the following observations can be made:

(1) If z is a complex number representing a point in the right half plane, f(z) is a point interior to the unit circle, i.e., f maps the right half plane to the interior of the unit circle.

(2) If z is a complex number representing a point in the left half plane (except the point -1), then $f(z)$ is a point ____, i.e., f maps the left half plane ____.

(3) If z is a complex number representing a point on the imaginary axis, then $f(z)$ is a point ____, i.e., f maps the imaginary axis ____.

ANSWER:

(2) exterior to the unit circle;
to the exterior of the unit circle.

(3) on the unit circle;
to the unit circle.

Note that $f(z) = 1$ holds for no complex number z.

Solve the inequality $\left|\frac{z - i}{z + i}\right| < 1$.

ANSWER:

$$
\begin{aligned}
\left|\frac{z - i}{z + i}\right| < 1 \quad &\Longleftrightarrow \quad z \neq -i \text{ and } |z - i| < |z + i| \\
&\Longleftrightarrow \quad z \neq -i \text{ and } |z - i| < |z - (-i)| \\
&\Longleftrightarrow \quad z \text{ is nearer } i \text{ than } -i \\
&\Longleftrightarrow \quad z \text{ is in the upper half plane (above the x-axis)} \\
&\Longleftrightarrow \quad \text{imaginary part of } z > 0.
\end{aligned}
$$

Analyze the function f defined by $f(z) = \frac{z - i}{z + i}$ as was done for the previous example.

ANSWER:

f maps the upper half plane to the interior of the unit circle.

f maps the lower half place (except the point $-i$) to the exterior of the unit circle.

f maps the real axis to the unit circle.

Note: $f(z) = 1$ holds for no complex number z.

- -

Let f be the function defined by $f(z) = 1/z$, for each non-zero complex number z.

If z is a point within the unit circle (except 0), where is $f(z)$?

- -

ANSWER:

$f(z)$ is a point outside the unit circle.

- -

In terms of mapping, f maps the interior of the unit circle (except 0) to the exterior of the unit circle.

Make a similar analysis for points on the unit circle.

- -

ANSWER:

If z is a point on the unit circle, $f(z)$ is a point on the unit circle, (or f maps the unit circle to the unit circle).

- -

Make a similar analysis for points outside the unit circle.

- -

ANSWER:

If z is a point outside the unit circle, $f(z)$ is a point inside the unit circle; or f maps the exterior of the unit circle to the interior of the unit circle.

- -

It should be pointed out that one important property of the field of real numbers does not carry over to the field of complex numbers.

The field of complex numbers is not an ordered field. We can show this by making the following observations:

If C were ordered, then by Order Theorem 4.13 the square of every non-zero element would be ____; in particular $i^2 = -1$ would be ____. But by Order Theorem 4.13, 1 is ____ and by Order Theorem 4.5, -1 is ____. This contradiction shows that C is not ordered.

- -

ANSWER:

positive (greater than zero);
positive (greater than zero).
positive (greater than zero)
negative (less than zero).

- -

REVIEW ITEMS

Items 1 - 4 refer to the following complex numbers,

(a) $1/i$, (b) 2, (c) i^3, (d) $\frac{2 + 3i}{1 + 4i}$.

1. Write each complex number as an ordered pair of real numbers and in the form $a + bi$ with real numbers a and b.

- -

ANSWER:

(a) $1/i = (0,-1) = 0 + (-1)i$
(b) $2 = (2, 0) = 2 + 0i$
(c) $i^3 = (0, -1) = 0 + (-1)i$
(d) $\frac{2 + 3i}{1 + 4i} = (14/17, - 5/17) = 14/17 + (- 5/17)i$

- -

2. What are the real part and the imaginary part of each complex

number?

- -

ANSWER:

(a) Real part of $1/i = 0$ Imaginary part of $1/i = -1$

(b) Real part of $2 = 2$ Imaginary part of $2 = 0$

(c) Real part of $i^3 = 0$ Imaginary part of $i^3 = -1$

(d) Real part of $\frac{2 + 3i}{1 + 4i} = \frac{14}{17}$ Imaginary part of $\frac{2 + 3i}{1 + 4i} = -\frac{5}{17}$

- -

3. What is the absolute value of each complex number?

- -

ANSWER:

(a) $|1/i| = 1$

(b) $|2| = 2$

(c) $|i^3| = 1$

(d) $\left|\frac{2 + 3i}{1 + 4i}\right| = \frac{\sqrt{221}}{17}$

- -

4. What is the conjugate of each complex number?

- -

ANSWER:

(a) $\overline{1/i} = i$

(b) $\overline{2} = 2$

(c) $\overline{i^3} = i$

(d) $\overline{\left(\frac{2 + 3i}{1 + 4i}\right)} = \frac{14}{17} + \frac{5}{17}i$

- -

5. Write the product $(2 + i)(1 + 3i)$ in the form $a + bi$, with real numbers a and b.

- -

ANSWER:

$(2 + i)(1 + 3i) = -1 + 7i$

- -

6. Where are the points in the plane which correspond to complex numbers with absolute value 5?

- -

ANSWER:

On the circle with center at the origin and radius 5.

- -

7. Where are the points in the plane which correspond to complex numbers z such that $|z + 5| < |z - 5|$?

- -

ANSWER:

In the left half plane.

$|z + 5| < |z - 5| \iff |z - (-5)| < |z - 5|$

$\iff$ z is closer to -5 than to 5

$\iff$ Real part of z is less than 0.

- -

8. Show that if z is a complex number then $\frac{z + \overline{z}}{2}$ is the real part of z.

- -

ANSWER:

Let $z = a + bi$, where a and b are real.

Then $\overline{z} = a - bi$.

$z + \overline{z} = a + bi + a - bi = 2a$

$\frac{z + \overline{z}}{2} = a =$ real part of z.

- -

ALGEBRA OF REAL FUNCTIONS

In this unit and the one following, we will make a fairly systematic study of polynomials and polynomial functions. Many high school texts use the term polynomial in a different sense from that used by practically all mathematicians today. In the word polynomial, the prefix poly- has the connotation of many and the stem -nomial represents term. Perhaps for this reason, the word polynomial is commonly used in high school texts to denote an algebraic expression with two or more terms. However, for practically all mathematicians today the word has a precise technical meaning which is related to the above but different in certain important respects. For example, the algebraic expressions $2x$, 5, $-3x^3$, 0 are not usually called polynomials in high school algebra texts but are polynomials according to the definition which we will adopt here. On the other hand such expressions as $\sqrt{7x} + 2$ and $1/x + 3x^2 - 5$ are often called polynomials by high school algebra texts but are not polynomials according to our definition. We will give precise definitions of the terms polynomial and polynomial function later, but first we wish to study somewhat more general classes of functions and algebraic systems which are formed by these functions. Many of the ideas introduced in the study of these systems will be used later in the study of polynomial functions.

Let us recall from Unit I some things about functions. Let f be the function defined by $f(x) = x^2$, for each real number x.

The domain of f is the set of ____.

- -

ANSWER:

real numbers.

- -

We say that f is a function ____ the set of real numbers ____ the set of real numbers.

- -

ANSWER:

from; to.

- -

What is the range of the function f described above?

- -

ANSWER:

The set of non-negative real numbers.

- -

In general, when we say that f is a function from the set of real numbers to the set of real numbers we mean that the ____ of f is the set of real numbers and the range of f is _____.

- -

ANSWER:

domain; a subset of the set of real numbers.

- -

Let X be a non-empty set. In the beginning we make no special assumptions about X. Later we will look at special cases where X is chosen to be a particular set, e.g., the set of real numbers, a finite set, etc. Let F denote the set of all functions from X to the real numbers. If f is a function in F, then the domain of f

478

is ____ and the range of f is ____.

ANSWER:

X

a subset of the set of real numbers.

If x is in X and f is in $\mathcal{F}$ then $f(x)$ is ____.

ANSWER:

a real number

If f and g are functions in the set $\mathcal{F}$, then $f = g$ if and only if $f(x) = g(x)$ for every element x in X.

We should emphasize that the set $\mathcal{F}$ is a set of functions and not a set of real numbers.

It is possible to define in a natural way two binary operations on $\mathcal{F}$, which we call addition and multiplication. We will use the usual symbols "+" and "·" for these operations.

DEFINITION 12.1: If f and g are functions in $\mathcal{F}$, then $f + g$ is defined to be the function h such that

$h(x) = f(x) + g(x)$, for each x in X,

and $f \cdot g$ is defined to be the function k such that

$k(x) = f(x) \cdot g(x)$, for each x in X.

In Definition 12.1, the elements $f(x) + g(x)$ and $f(x) \cdot g(x)$ belong to what set?

ANSWER:

The set of real numbers.

The elements $f + g$ and $f \cdot g$ are ____ from X to the set of real numbers.

ANSWER:

functions.

Therefore $f + g$ and $f \cdot g$ are elements of the set ____.

ANSWER:

F.

You should be careful to note here that the symbols "$f(x)$", "$g(x)$", etc., do not represent functions but represent real numbers which are paired with the element x by the functions f, g, etc. For every element x in X there is an ordered pair $(x, f(x))$ in f and an ordered pair $(x, g(x))$ in g. If $h = f + g$ and $k = f \cdot g$ then in the function h there will be the ordered pair $(x, h(x)) =$ $(x,$ ____$)$ and in the function k there will be the ordered pair $(x, k(x)) = (x,$ ____$)$.

ANSWER:

$f(x) + g(x)$; $f(x) \cdot g(x)$.

If the ordered pair $(x, 5)$ is in f and the ordered pair $(x, -2)$ is in g then the ordered pair $(x,$ ___$)$ is in $f + g$ and the ordered pair $(x,$ ___$)$ is in $f \cdot g$.

ANSWER:

3; -10

- -

For an example, let X = {a, b, c}. The elements of X are the letters a, b, c. Let f and g be the functions from X to R (the set of real numbers) whose ordered pairs are listed as follows:

f	g	f + g	f · g
(a, 2)	(a, 3)	____	____
(b, -3/2)	(b, 0)	____	____
(c, $\sqrt{5}$)	(c, -15)	____	____

Fill in the blanks with the ordered pairs in f + g and f · g.

- -

ANSWER:

f + g	f · g
(a, 5)	(a, 6)
(b, -3/2)	(b, 0)
(c, $\sqrt{5}$ -15)	(c, $-15\sqrt{5}$)

- -

Let us consider the above with an alternate notation.

f: $a \xrightarrow{f} 2$
$b \xrightarrow{f} -3/2$
$c \xrightarrow{f} \sqrt{5}$

g: $a \xrightarrow{g} 3$
$b \xrightarrow{g} 0$
$c \xrightarrow{g} -15$

f + g: $a \xrightarrow{f+g} 5$
$b \xrightarrow{f+g} -3/2$
$c \xrightarrow{f+g} \sqrt{5} - 15$

f · g: $a \xrightarrow{f \cdot g} 6$
$b \xrightarrow{f \cdot g} 0$
$c \xrightarrow{f \cdot g} -15\sqrt{5}$

Using this notation describe f + g and f · g where f: $a \xrightarrow{f} -\sqrt{3}$ g: $a \xrightarrow{g} \sqrt{3}$ f + g: ____ f · g: ____

$b \xrightarrow{f} \pi$ $b \xrightarrow{g} 13$ ____ ____

$c \xrightarrow{f} 32$ $c \xrightarrow{g} 0$ ____ ____

- -

ANSWER:

f + g: $a \xrightarrow{f+g} 0$ f g: $a \xrightarrow{f \cdot g} -3$

$b \xrightarrow{f+g} \pi + 13$ $b \xrightarrow{f \cdot g} 13\pi$

$c \xrightarrow{f+g} 32$ $c \xrightarrow{f \cdot g} 0$

- -

If x is in X then $x \xrightarrow{f} f(x)$, $x \xrightarrow{g} g(x)$, $x \xrightarrow{f+g}$ ____ and $x \xrightarrow{f \cdot g}$ ____

- -

ANSWER:

$f(x) + g(x)$; $f(x) \cdot g(x)$.

- -

For another example, let X be the set of complex numbers. Let f and g be functions from X to R defined by

$f(x) = |x|$, for each complex number x,

$g(x) =$ the real part of x, for each complex number x.

Fill in the following blanks:

$2 + i \xrightarrow{f}$ ____ $-3i \xrightarrow{f}$ ____

$2 + i \xrightarrow{g}$ ____ $-3i \xrightarrow{g}$ ____

$2 + i \xrightarrow{f+g}$ ____ $-3i \xrightarrow{f+g}$ ____

$2 + i \xrightarrow{f \cdot g}$ ____ $-3i \xrightarrow{f \cdot g}$ ____

- -

ANSWER:

$2 + i \xrightarrow{f} \sqrt{5}$

$2 + i \xrightarrow{g} 2$

$2 + i \xrightarrow{f+g} \sqrt{5} + 2$

$2 + i \xrightarrow{f \cdot g} \sqrt{5} \cdot 2$

$-3i \xrightarrow{f} 3$

$-3i \xrightarrow{g} 0$

$-3i \xrightarrow{f+g} 3 + 0 = 3$

$-3i \xrightarrow{f \cdot g} 3 \cdot 0 = 0$

It is almost obvious from the definitions that addition and multiplication in F have many of the properties of addition and multiplication of real numbers (associative properties, commutative properties, etc.). However, we will go through the proofs of some of these.

Property A_a for F would state: if f, g, and h are functions in the set F, then $(f + g) + h =$ _____.

ANSWER:

$f + (g + h)$.

If f, g, and h are functions in F, then

$[(f + g) + h](x) = (f + g)(x) + h(x) = [f(x) + g(x)] + h(x)$.

$[f + (g + h)](x) =$ _____.

ANSWER:

$f(x) + (g(x) + h(x))$.

Let f, g, and h be functions in F. To show that $(f + g) + h = f + (g + h)$, we have to show that for each element x in X, the real number paired with x by the function $(f + g) + h$ is the same as the real number paired with x by the function $f + (g + h)$.

This can be stated

$[(f + g) + h](x) = [f + (g + h)](x)$.

However, this notation is a little unwieldy.

By definition of addition in F

$f + g: x \longrightarrow$ _____.

- -

ANSWER:

$f(x) + g(x)$.

- -

Therefore

$(f + g) + h: x \longrightarrow$ _____.

- -

ANSWER:

$[f(x) + g(x)] + h(x)$

- -

Thus, if we let $k = (f + g) + h$, then $k(x) =$ _____.

- -

ANSWER:

$[f(x) + g(x)] + h(x)$

- -

Similarly,

$f + (g + h): x \longrightarrow$ _____.

- -

ANSWER:

$f(x) + [g(x) + h(x)]$

- -

$[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$ because of Property ____ of the real numbers.

- -

ANSWER:

A_a.

- -

This proves that $(f + g) + h = f + (g + h)$.

In the equation

$[(f + g) + h](x) = [f(x) + g(x)] + h(x)$,

(a) $f + g$ and $(f + g) + h$ are elements of the set ____.

(b) $f(x) + g(x)$ and $[f(x) + g(x)] + h(x)$ are elements of the set ____.

(c) x is an element of the set ____.

- -

ANSWER:

(a) F, (b) of real numbers, (c) X.

- -

State the Property A_c for F.

- -

ANSWER:

If f and g are functions in the set F then $f + g = g + f$.

- -

Criticize the answer, "$f(x) + g(x) = g(x) + f(x)$" for the preceding item.

- -

ANSWER:

$f(x)$ and $g(x)$ are real numbers and not elements of the set F. However, the statement "$f(x) + g(x) = g(x) + f(x)$" _is true_ for

485

each element x in X, because Property A_c is true for the system of real numbers.

Prove that Property A_c holds for F. Give a reason for each step in your proof.

ANSWER:

If f and g are functions in F and x is in X, then

$$\left.\begin{array}{l} (f+g)(x) = f(x)+g(x) \\ \text{and} \\ (g+f)(x) = g(x)+f(x) \end{array}\right\} \quad \text{by definition of addition in } F$$

$$f(x)+g(x) = g(x)+f(x) \quad \text{by Property } A_c \text{ for the real numbers.}$$

Since $(f+g)(x) = (g+f)(x)$ for each x in X, $f+g = g+f$, because of the way equality of functions is defined.

$$\left.\begin{array}{l} f+g:\ x \longrightarrow f(x)+g(x) \\ g+f:\ x \longrightarrow g(x)+f(x) \end{array}\right\} \quad \text{by definition of addition}$$

$$f(x)+g(x) = g(x)+f(x) \quad \text{by Property } A_c \text{ for the real numbers.}$$

Therefore $f+g$ and $g+f$ pair up the same real number with x, for each x in X. Then $f+g = g+f$.

Is the number zero an additive identity for F? Explain.

ANSWER:

No. The number zero is not in the set F. An additive identity for F must be an element of F; i.e., a function from X to the set of real numbers.

What is the additive identity for F?

____.

- -

ANSWER:

The function f defined by $f(x) = 0$, for each x in X; or the function f defined by $f: x \longrightarrow 0$, for each x in X. If you said "$f(x) = 0$" you should count your answer incorrect since you have not completely defined the function f.

- -

We call this function the zero function. Property A_{id} holds in F. What is the additive inverse of a function f in F?

____.

- -

ANSWER:

The function g defined by $g(x) = -f(x)$, for each x in X. If you said $-f(x)$ you should count your answer as incorrect. $-f(x)$ is a real number. The additive inverse of f must be an element of F; i.e., a function from X to the set of real numbers. Also if you said "$g(x) = -f(x)$", you should count your answer as incorrect since you have not completely defined the function g.

- -

We will denote this function g by $-f$. Thus $-f$ is an element of the set ____ with the property that $-f + f = f + (-f) =$ ____.

- -

ANSWER:

F; the zero function in F. (not the number zero).

- -

If x is in X, then $(-f)(x) = -f(x)$ and $-f(x)$ is in the set

____.

- -

ANSWER:

of real numbers.

- -

We see that Property A_{in} holds in F. Is F closed under subtraction?

- -

ANSWER:

Yes.

- -

State Property M_a for F.

- -

ANSWER:

If f, g, and h are functions in F, then $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

- -

Prove that Property M_a holds in F. Give a reason for each step in your proof. [Hint: Use as a guide the proof that Property A_a holds.]

- -

ANSWER:

If f, g, and h are in F, and if x is in X, then $[(f \cdot g) \cdot h](x) = (f \cdot g)(x) \cdot h(x) = [f(x) \cdot g(x)] \cdot h(x)$, by definition and

$[f \cdot (g \cdot h)](x) = f(x) \cdot (g \cdot h)(x) = f(x) \cdot [g(x) \cdot h(x)]$, by definition.

$[f(x) \cdot g(x)] \cdot h(x) = f(x) \cdot [g(x) \cdot h(x)]$, by property M_a for the real numbers.

Therefore $[(f \cdot g) \cdot h](x) = [f \cdot (g \cdot h)](x)$ for each x in X, which means that $(f \cdot g) \cdot h = f \cdot (g \cdot h)$, because of the way equality of functions is defined.

- -

M_c also holds in F. What is the multiplicative identity in F?

- -

ANSWER:

The function f defined by: $f(x) = 1$, for each x in X. If you said "the number 1," your answer is incorrect. The number 1 is not an element of F. The multiplicative identity for F must be an element of F; i.e., a function from X to the set of real numbers. Also, the answer "$f(x) = 1$" is not complete.

- -

Therefore Property M_{id} holds in F. If f is a function in F, and if f has a multiplicative inverse g, then

$g(x) =$ _____, for each x in X.

- -

ANSWER:

$1/f(x)$, or $f(x)^{-1}$.

- -

For an example, let X be the set of real numbers and let f be defined by:

$f(x) = |x|$, for each real number x.

What is wrong with the following? Let g be the function defined by:

$g(x) = 1/|x|$, for each real number x.

- -

ANSWER:

$1/|x|$ has no meaning when x is the real number 0.

Does the function f defined in the example above have a multiplicative inverse in F?

ANSWER:

No.

We see that a function f in F has a multiplicative inverse if and only if ____ for each x in X.

ANSWER:

$f(x) \neq 0$.

If X contains more than one element then we can find a function f in F such that $f(x) = 0$ for some x in X and $f(x) \neq 0$ for some other element x in X. Such a function would not be the zero function. Would it have a multiplicative inverse?

ANSWER:

No, since $f(x) = 0$ for some x in X. (We emphasize that f is in F but f has no multiplicative inverse in F.)

Suppose the set X has just one element, say $X = \{a\}$. A function f in F is non-zero only if $f(a)$ ____.

ANSWER:

$\neq 0$.

- -

If $f(a) \neq 0$, then f has a multiplicative inverse in F, the function g defined by $g(a) =$ ____.

- -

ANSWER:

$1/f(a)$, or $f(a)^{-1}$.

- -

If $X = \{a\}$ has only one element then if f is in F and $f(a) = 0$, f is the zero function.

We see that Property M_{in} holds in F if and only if ____.

- -

ANSWER:

X contains only one element. (Remember that Property M_{in} does not require that the zero function (the additive identity) have an inverse).

- -

In general, F possesses all the defining properties (postulates) of a field except for Property M_{in}. Since F does not have Property M_{in}, we cannot always perform the division operation in F.

Consider the example where X is the set of real numbers. Let f and g be defined by

$f(x) = 2x^2$, for each real number x.

$g(x) = 1 - x^2$, for each real number x.

For what real numbers x does $\frac{f(x)}{g(x)}$ have meaning?

- -

491

ANSWER:

All real numbers except 1 and -1.

- -

Let h be the function defined by

$h(x) = \frac{2x^2}{1 - x^2}$ for each real number x such that $1 - x^2 \neq 0$.

What is the domain of h?

- -

ANSWER:

The set of real numbers x for which $1 - x^2 \neq 0$; i.e., the set of real numbers different from 1 and -1.

- -

What is the domain of each function in F?

- -

ANSWER:

X (in this example, X is the set of real numbers.)

- -

Is the function h in F?

- -

ANSWER:

No.

- -

In general, we can define an operation in F which is somewhat like division. Thus if f and g are in F and g is not the zero function, then there is a function h defined by $h(x) = \frac{f(x)}{g(x)}$, for each x in X such that $g(x) \neq 0$.

Is h necessarily in F? Why?

- -

ANSWER:

No, the domain of h may not be all of X, since the domain of h cannot contain any real number x for which $g(x) = 0$.

Is this operation of division closed in F?

ANSWER:

No.

The operations of addition and multiplication of functions which we have defined in this unit should not be confused with the operation of composition of functions which we defined in Unit I. Let us consider each of these three operations on the set of all functions from the real numbers to the real numbers.

Let $f(x) = 2x + 1$, for each real number x,
and $g(x) = x^2$, for each real number x,

then

(a) $f + g\colon x \to$ _____, for each real number x,
(b) $f \cdot g\colon x \to$ _____, for each real number x,
(c) $f \circ g\colon x \to$ _____, for each real number x,
(d) $g \circ f\colon x \to$ _____, for each real number x.

ANSWER:

(a) $x^2 + 2x + 1$, (b) $2x^3 + x^2$, (c) $2x^2 + 1$, (d) $(2x + 1)^2$.

There may be some confusion concerning the three functions which serve as identity elements for these three operations. These are the functions f, g, and h defined as follows:

(a) addition: $f(x) =$ _____, for each real number x,

(b) multiplication: $g(x) =$ _____, for each real number x,

(c) composition: $h(x) =$ _____, for each real number x.

- -

ANSWER:

(a) 0,

(b) 1,

(c) x.

- -

When we speak of the identity function on the set of real numbers we usually mean the function which is the identity element for composition of functions; i.e., the function h defined by: $h(x) = x$, for each real number x.

Also recall that the symbol f^{-1} is used to denote the inverse of a function f with respect to the operation ____ of functions.

- -

ANSWER:

composition.

- -

The inverse of f with respect to addition is denoted by $-f$. In general, f does not have an inverse with respect to multiplication. When f does have an inverse with respect to multiplication it is sometimes denoted by $1/f$.

Let us recall the definition of isomorphism given in Unit III. If G_1 is a group under an operation "*" and G_2 is a group under an operation "o" then G_1 is isomorphic to G_2 if there is a function ϕ with the following three properties:

(a) ϕ is a function from G_1 ____ G_2,

(b) ϕ is a(n) _____ function, and

(c) $\phi\ (a * b) =$ ____, for all elements a, b in G_1.

ANSWER:

(a) onto;

(b) reversible,

(c) $\phi(a) \circ \phi(b)$.

We call the function ϕ an isomorphism from G_1 onto G_2.

Suppose K_1 and K_2 are fields. (We denote the two operations in K_1 and in K_2 by "+" and "·".) Then an isomorphism of K_1 onto K_2 is a reversible function ϕ from K_1 onto K_2 such that

____ for all elements a, b in K_1, and

____ for all elements a, b in K_1.

ANSWER:

$\phi(a + b) = \phi(a) + \phi(b)$,

$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Now, let X be the set $\{0, 1\}$ and let F be the set of all functions from X to the set of real numbers. Let ϕ be the function defined by

$\phi(f) = f(1)$, for each element f in F.

What is the domain of ϕ?

ANSWER:

F.

ϕ is a function from F to ____.

ANSWER:

the set of real numbers.

- -

Let f be the function in F defined by:

$f(0) = 13$, $f(1) = -\sqrt{3}$.

What is $\phi(f)$?

- -

ANSWER:

$-\sqrt{3}$

- -

Suppose k is a real number. Find a function f in F such that $\phi(f) = k$.

- -

ANSWER:

Any function f such that $f(1) = k$; i.e., $f(0)$ can be any real number and $f(1) = k$. If you said only "$f(1) = k$", your answer is not complete.

- -

What is the range of the function ϕ?

- -

ANSWER:

The set of all real numbers.

- -

If f and g are functions in F, what is $\phi(f + g)$?

- -

ANSWER:

$(f + g)(1)$, or $f(1) + g(1)$.

- -

What is $\phi(f) + \phi(g)$?

- -

ANSWER:

$f(1) + g(1)$.

- -

Does $\phi(f + g) = \phi(f) + \phi(g)$ for all elements f and g in F?

- -

ANSWER:

Yes.

- -

We have shown that ϕ is a function from F onto the set of real numbers such that

$\phi(f + g) = \phi(f) + \phi(g)$, for all elements f, g in F.

Similarly, we can show that

$\phi(f \cdot g) = \phi(f) \cdot \phi(g)$, for all elements f, g in F.

What else would we need to show about ϕ to be able to conclude that ϕ is an isomorphism from F onto R?

- -

ANSWER:

That ϕ is reversible.

- -

Consider the functions f and g in F defined by: $f(0) = 1$, $f(1) = 5$; $g(0) = 3$, $g(1) = 5$.

What are $\phi(f)$ and $\phi(g)$?

ANSWER:

$\phi(f) = 5$, $\phi(g) = 5$.

Is ϕ a reversible function?

ANSWER:

No. $f \neq g$ but $\phi(f) = \phi(g)$, where f and g are the functions defined in the preceding item.

A function from one algebraic system to another which preserves the operations but which may not be reversible is often called a homomorphism. The function ϕ above is a homomorphism from F onto R.

Return now to our original assumption that X is a set and F is the algebraic system of all functions from X to the set of real numbers. Let x_0 be an element of X. Let ϕ be the function defined by

$\phi(f) = f(x_0)$, for each element f in F.

What is the domain of ϕ?

ANSWER:

F.

ϕ is a function from F to ____ .

ANSWER:

the set of real numbers.

Is the range of ϕ the set of all real numbers?

ANSWER:

Yes. If k is a real number, there is a function f in F such that $f(x_0) = k$; then $\phi(f) = k$.

If f and g are elements of F, what is $\phi(f + g)$?

$\phi(f) + \phi(g)$?

ANSWER:

$\phi(f + g) = (f + g)(x_0) = f(x_0) + g(x_0)$.

$\phi(f) + \phi(g) = f(x_0) + g(x_0)$.

Does $\phi(f + g) = \phi(f) + \phi(g)$ for all elements f and g in F?

ANSWER:

Yes.

Similarly, $\phi(f \cdot g) = \phi(f) \cdot \phi(g)$ for all elements f and g in F.

Thus ϕ is a(n) ____ from F onto R.

ANSWER:

homomorphism.

- -

Is there a condition on X which will ensure that ϕ is reversible? What is it?

- -

ANSWER:

Yes. If X contains only one element.

- -

DEFINITION 12.2: A function f in F is called a constant function if its range consists of a single element.

If f is a constant function with range $\{a\}$ and g is a constant function with range $\{b\}$ what is the range of $f + g$ ____, of $f - g$ ____, of $f \cdot g$? ____

- -

ANSWER:

$\{a + b\}$, $\{a - b\}$, $\{a \cdot b\}$.

- -

Is the set K of all constant functions closed under addition, subtraction, and multiplication? _____.

- -

ANSWER:

Yes.

- -

We saw that property M_{in} does not hold in F, in general. If f is a non-zero constant function in F does f have a multiplicative inverse in F?

- -

ANSWER:

Yes.

If f is a non-zero constant function in $\mathcal{F}$ with range $\{a\}$, then $a \neq 0$ and the multiplicative inverse g of f is defined by:

ANSWER:

$g(x) = 1/a$, for each x in X.

The set of non-zero constant functions in $\mathcal{F}$ is closed under division. Let x_0 be an element of X. Let ψ be the function defined by

$\psi(f) = f(x_0)$, for each f in $\mathcal{K}$.

The domain of ψ is ____.

ANSWER:

$\mathcal{K}$.

[Note that the function ψ is defined just as we defined the function ϕ previously except that the domain of ϕ was $\mathcal{F}$ and the domain of ψ is $\mathcal{K}$.]

What is the range of ψ?

ANSWER:

The set of all real numbers.

Does $\psi(f + g) = \psi(f) + \psi(g)$ for all elements f and g in K?

- -

ANSWER:

Yes.

- -

Also, $\psi(f \cdot g) = \psi(f) \cdot \psi(g)$ for all elements f and g in K.

Suppose f and g are functions in K and $f(x_0) = g(x_0)$. If x is any element of X, then $f(x) = f(x_0)$ and $g(x) = g(x_0)$. Why?

- -

ANSWER:

f and g are constant functions.

- -

If $\psi(f) = \psi(g)$, does $f = g$?

- -

ANSWER:

Yes.

- -

We conclude that ψ is a(n) ____ function from K onto R which preserves the operations. Therefore ψ is a(n) ____ from K onto R.

- -

ANSWER:

reversible; isomorphism.

- -

A special case in our discussion which is of particular interest is that in which $X = R$ (the set of real numbers). In this case a function in F has domain X = ____ and range ____.

ANSWER:

R; a subset of R.

Let f and g be functions defined by

$f(x) = 3x^2$, for each real number x,
$g(x) = \sqrt[3]{x} + 1$, for each real number x.

Then, for each real number x,

$(f + g)(x) =$ ____, and
$(f \cdot g)(x) =$ ____.

ANSWER:

$3x^2 + \sqrt[3]{x} + 1$; $3x^2\sqrt[3]{x} + 3x^2$

If $x \xrightarrow{f} 2x - 1$ and $x \xrightarrow{g} x^2 + 1$, for each real number x, then $1 \xrightarrow{f+g}$ ____, $3 \xrightarrow{f \cdot g}$ ____, and $-1 \xrightarrow{f-g}$ ____.

ANSWER:

3; 50; -5.

POLYNOMIAL FUNCTIONS

A real polynomial function is a special kind of function from the real numbers to the real numbers. The simplest polynomial functions are the constant functions. Every constant function from the set of real numbers to the set of real numbers is a polynomial function.

Let f be the function defined by $f(x) = 5$, for each real number x; f is a constant polynomial function.

What is the domain of f?

ANSWER:

The set of real numbers.

What is the range of f?

ANSWER:

The set $\{5\}$.

How many elements can the range of a constant polynomial function contain?

ANSWER:

Only one.

The identity function on R is a polynomial function. The range of the identity polynomial function is ____.

ANSWER:

the set of real numbers.

We have seen that the set F consisting of all functions f such that the domain of f is the set of real numbers and the range of f is a subset of the set of real numbers is closed under addition, subtraction, and multiplication, but not under division. Are the constant polynomial functions and the identity polynomial function in F?

- -

ANSWER:

Yes.

- -

Every real polynomial function can be obtained from the identity function and the constant functions by a finite number of additions and multiplications. Consider the function f defined by $f(x) = -5x^2$, for each real number x. f is a polynomial function. It can be obtained by multiplying the square of the ____ function and the constant function g defined by ____.

- -

ANSWER:

identity; $g(x) = -5$, for each real number x.

Note: Did you forget to include the phrase "for each real number x"? Remember that to define the function g by the rule "$g(x) = -5$" we must also specify the domain of the function --- in this case the set of real numbers.

- -

DEFINITION 12.3: If $\underline{a}$ is a real number and n is a non-negative integer, and if $f(x) = ax^n$, for each real number x, then f is called a monomial function.

Every monomial function is a polynomial function.

The function g, defined by $g(x) = 2x^3 + 3x^2 - 5x + 2$, for each real number x, can be obtained by ____ four monomial functions.

- -

ANSWER:

adding.

Every polynomial function is either a monomial function or the sum of a finite number of monomial functions. We now give a precise definition of polynomial function.

DEFINITION 12.4: A real polynomial function is a function f whose domain is ____ and for which there is a non-negative integer n and a sequence $(a_0, a_1, a_2, \ldots, a_n)$ of ____ such that $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, for each real number x.

ANSWER:

the set of real numbers; real numbers.

The rule $f(x) = 2x^{-2} + 3x^{-1} + 5$ is not of the kind given in Definition 12.4 because -2 and -1 are not ____.

ANSWER:

non-negative integers.

Similarly, such rules as $f(x) = \sqrt{x} - x^{\frac{1}{2}}$ are excluded.

Is the set of polynomial functions closed under addition? ____, subtraction? ____, multiplication? ____, division? ____.

ANSWER:

yes; yes; yes; no.

The polynomial functions from a subsystem of the system F of all functions from R to R.

In this unit we have been concerned almost exclusively with functions from a set X to the set of real numbers. The algebra of such functions has been built up on the basis of the field properties of the real numbers. We could go back and obtain a parallel development by replacing the system of real numbers with an arbitrary field; e.g., the field of rational numbers, the field of complex numbers, the field I/3, the field I/5, etc. Thus if K is any field we could concern ourselves with functions from a set X to K. We will not repeat the details of such a development here but we will use later some of the ideas presented here for fields other than the real number system.

REVIEW ITEMS

1. Let F be the set of all functions from a set X to the real numbers. If h = f + g, then h(x) = f(x) + g(x), for each element x in X.

(a) f + g is an element of what set?
(b) f(x) + g(x) is an element of what set?
(c) x is an element of what set?
(d) h(x) is an element of what set?

- -

ANSWER:

(a) F.
(b) Set of real numbers.
(c) X.
(d) Set of real numbers.

- -

2. Let f and g be functions defined by

$f(x) = 2x^2 + 3$, for each real number x,
$g(x) = \sqrt{x^2 + 1}$, for each real number x.

(a) $f + g: 2 \longrightarrow \underline{\qquad}$.
(b) $f \cdot g: 2 \longrightarrow \underline{\qquad}$.
(c) $f - g: 2 \longrightarrow \underline{\qquad}$.
(d) $f \circ g: 2 \longrightarrow \underline{\qquad}$. ($f \circ g$ is the composite of f with g.)

ANSWER:

(a) $11 + \sqrt{5}$.
(b) $11\sqrt{5}$.
(c) $11 - \sqrt{5}$.
(d) 13.

---

3. Let F be the set of all functions from the set of complex numbers to the set of real numbers. Let f be defined by

$f(x) = |x|$, for each real number x.

Does f have a multiplicative inverse in F? Explain.

ANSWER:

No, if g is a multiplicative inverse for f, then $g(x) = 1/|x|$, for each complex number x. This is impossible because $1/|x|$ has no meaning when $x = 0$.

---

4. Prove that property M_c is valid in the system F of all functions from a set X to the real numbers. Give a reason for each step in your proof.

ANSWER:

We must prove that if f and g are functions in F, then $f \cdot g = g \cdot f$.

(1) $f \cdot g\colon x \longrightarrow f(x) \cdot g(x)$, for each real number x.

(2) $g \cdot f\colon x \longrightarrow g(x) \cdot f(x)$, for each real number x.

(3) $f(x) \cdot g(x) = g(x) \cdot f(x)$, for each real number x.

(4) Therefore $f \cdot g = g \cdot f$.

(1) By definition of multiplication in F.

(2) By definition of multiplication in F.

(3) By property M_c for real numbers.

---

5. Let F be the set of all functions from the set of positive integers to the set of real numbers. Let ϕ be the function from F to the real numbers defined by

$\phi\colon f \longrightarrow f(2)$, for each element f in F.

(a) What is the domain of ϕ?

(b) What is the range of ϕ?

(c) Let f be defined by

$f(x) = x^2$, for each positive integer x.

What is $\phi(f)$ in this case?

(d) If f and g are elements of F, what is $\phi(f + g)$?

(e) Is $\phi(f + g)$ the same as $\phi(f) + \phi(g)$?

ANSWER:

(a) F.

(b) The set of real numbers.

(c) $\phi(f) = f(2) = 2^2 = 4$.

(d) $\phi(f + g) = (f + g)(2) = f(2) + g(2)$.

(e) Yes: $\phi(f) + \phi(g) = f(2) + g(2)$.

---

6. Refer to the preceding item. Give different functions f and g such that $\phi(f) = \phi(g)$.

ANWSER:

There are many possible correct answers. For example:

f: $x \longrightarrow x^2$, for each positive integer x.

g: $x \longrightarrow 2x$, for each positive integer x.

In this case, $\phi(f) = f(2) = 2^2 = 4$, $\phi(g) = g(2) = 2 \cdot 2 = 4$.

7. What must be true about a set X if every function from X to the set of real numbers is a constant function?

ANSWER:

X has only one element.

8. The domain of a real polynomial function is ____, and the range is ____.

ANSWER:

The set of real numbers; a subset of the set of real numbers.

Note: To be correct, your second answer must contain the phrase "a subset of".

POLYNOMIALS

In the definition of real polynomial function given in the preceding unit we have required that the domain of such a function be the set of real numbers. Therefore a real polynomial function f defined by

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, for each real number x, is completely determined by the "algebraic expression"

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, in the variable x.

DEFINITION 13.1: A real polynomial is an algebraic expression of the form $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, where x is a variable, n is a non-negative integer, and $(a_0, a_1, \dots, a_n)$ is a sequence of real numbers.

More generally, we could define a "polynomial over K" for any field K by requiring that $a_0, a_1, \dots, a_n$ be elements of K. In the beginning we will state all our results for real polynomials. You may observe however that these results are dependent upon the field properties and can be restated for an arbitrary field K. Later in the unit we will be concerned with polynomials over fields different from the field of real numbers.

The expressions which we call polynomials are often called "polynomials in one variable" to distinguish them from similar expressions which involve two or more variables (e.g., $x^2 + 2xy + 3xy^2 - 4$ would be called a "polynomial in the two variables x and y").

We will be concerned, in this unit, only with polynomials in one variable.

Which of the following expressions are polynomials?

(a) $2x + 3$

(b) $x^3 - 3x^2 + 2x - 1$

(c) 3

(d) $1/x$

(e) $x^2 + 1/x$

(f) 0

ANSWER:

(a), (b), (c), (f)

Note that any real number may be expressed in the form given in Definition 13.1 and is therefore a polynomial. Such a polynomial is called a constant polynomial.

Let us examine some definitions which are commonly given for the word polynomial.

Example 1: One well-known high school text (the "Modern Mathematics Edition") defines polynomial in the following way: "Expressions which have one term are called monomials. Expressions which have two or more terms are called polynomials." This definition depends upon the meaning of the word term which is defined as follows: "An expression which either is a number or results in a number when the variable or variables in the expression are replaced by numbers is called a term. For example, $5ax$ is an expression having one term while $10a + 4$ is an expression having two terms: $10a$ and 4."

Consider the following questions that might be asked:

1. "$10a + 4$" is an expression which "results" in a number when the variable a is replaced by a number. Is it a term according to the

above definition? Do you think the authors intended that $10a + 4$ should be called a term?

2. In the expression $10a + 4$, 10 is a number. Is it a term according to the given definition?

3. In the definition of polynomial what is the meaning of the word "have"? According to the definition of term, 5, a, and x are each terms. Does the expression $5ax$ "have" the term 5, or a, or x?

4. Is $\sqrt{x}$ a term according to the definition? If we assume that the word "number" in the definitions refers to "real number", note that $\sqrt{x}$ does not seem to fit the definition of term since it does not "result" in a number when x is replaced by -1, for example. On the other hand $\sqrt[3]{x}$ does seem to fit the definition.

We will make no attempt to answer the above questions.

Example 2: The Ball State Curriculum materials define polynomial function in much the same way that we have in Unit XII. Then the term polynomial is used to mean polynomial function. Of particular importance in the development given in these materials is the following theorem, which is stated but not proved:

"Theorem 7.1 (The 'Uniqueness of Representation' Theorem for Polynomials). Two polynomial functions are identical if and only if their coefficient sets are identical, that is, if and only if the first coefficient of one is equal to the first coefficient of the other, etc."[1]

The statement is made that this theorem "is obvious, but very difficult to prove". One might take exception to the statement that the theorem is "obvious". The theorem is true for polynomials over a field with an infinite number of elements (any one of the number fields, for example) and a proof is given later in this unit. However, the theorem is not true for polynomials over a field with only a finite number of elements (the fields I/2, I/3, I/5, for example). Of course, in the Ball State materials only polynomials over the number fields are considered.

---

[1] Brumfiel, Eicholz, and Shanks, Algebra II. Addison-Wesley Publishing Co., Inc., Reading, Massachusetts, 1962, p. 209.

Example 3: The S.M.S.G. text defines polynomial as follows: "By a polynomial in x we mean an expression ... which is a sum of terms of the form

$a, bx, cx^2, dx^3, \ldots$

a, b, c, d, ... being numbers."[2]

This is essentially the definition that we have given.

In the definition of polynomial we have given no attempt is made to define the word "variable" or the phrase "algebraic expression". Near the end of this unit we will restate the definition of polynomial so that these terms do not appear. For the present it is sufficient to think of x as simply a symbol upon which we can perform certain elementary algebraic operations. We do emphasize that a variable is not a real number, not even an "unknown" one. Most of the properties of a variable which we need are contained in definitions which we will state presently. In connection with the foregoing remarks the student is urged to read Chapter 2 of A Concrete Approach to Abstract Algebra by W. W. Sawyer.[3]

Whatever meaning is attached to the word "variable" it is essential for our purposes that a polynomial be completely determined by its coefficients. More precisely we will assume as part of our definition of polynomial:

---

[2] School Mathematics Study Group, Intermediate Mathematics. Yale University Press, 1961, pp. 86-87.

[3] Sawyer, W. W. A Concrete Approach to Abstract Algebra. San Francisco: Freeman, 1959.

DEFINITION 13.2: The polynomial $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, with $a_n \neq 0$, is the same as the polynomial:

$b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, with $b_m \neq 0$, if and only if $n = m$ and $a_0 = b_0$, $a_1 = b_1$, ..., $a_n = b_n$.

DEFINITION 13.3: In the polynomial $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, the real numbers $a_0, a_1, \ldots, a_n$ are called coefficients of the polynomial. If $a_n \neq 0$, then a_n is called the leading coefficient, and the polynomial is said to be of degree n.

The polynomial $3x^2 - 2x + 1$ has leading coefficient ____ and degree ____.

- -

ANSWER:

3; 2.

- -

The polynomial 5 has leading coefficient ____ and degree ____.

- -

ANSWER:

5; 0.

- -

The degree of a non-zero polynomial is an element of the set of ____.

- -

ANSWER:

non-negative integers.

- -

The number zero is called the zero polynomial. It is a constant polynomial. We do not assign any degree to the zero polynomial. Be careful to note that this does not mean that the zero polynomial has degree zero. It has no degree at all.

What is the degree of each of the following polynomials?

(a) $2x + 3$

(b) 3

(c) $x^3 - 3x^2 + 2x - 1$

(d) 0

ANSWER:

(a) 1

(b) 0

(c) 3

(d) has no degree

What is the degree of a non-zero constant polynomial?

ANSWER:

zero

DEFINITION 13.4: The expressions a_nx^n, $a_{n-1}x^{n-1}$, ..., a_1x, a_0, in the polynomial $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ are monomials and are called terms of the polynomial.

Polynomials are equal if they have the same non-zero terms (terms with non-zero coefficients). In writing a non-zero polynomial we often omit the zero terms.

Consider the polynomial $x^5 + 3x^3 - x^2 + 2$.

(i) What is the degree of the polynomial?

(ii) What is the leading coefficient?

(iii) Is 2 a coefficient?

(iv) Is $3x^3$ a coefficient?

(v) $-x^2$ is a ____ of the polynomial.

ANSWER:

(i) 5

(ii) 1

(iii) yes

(iv) no

(v) term

ALGEBRA OF POLYNOMIALS

Addition and multiplication of polynomials are defined just as if the variable x were a real number, using the properties of addition and multiplication of real numbers. To make this clearer, let us suppose for the moment that x is a real number (not a variable) and consider the sum

$(2x^2 + 3x + 5) + (4x^2 + x + 2)$.

What properties of the real number system tell us that

$(2x^2 + 3x + 5) + (4x^2 + x + 2) = (2x^2 + 4x^2) + (3x + x) + (5 + 2)$?

ANSWER:

A_a and A_c, or associative and commutative properties for addition.

Using the ____ property for real numbers we have $(2x^2 + 4x^2) + (3x + x) + (5 + 2) = (2 + 4)x^2 + (3 + 1)x + 5 + 2 = 6x^2 + 4x + 7$.

ANSWER:

distributive (Property M_{id} is also used to replace x by $1 \cdot x$.)

Now consider the product

$(2x^2 + 3x + 5) \cdot (4x^2 + x + 2)$.

By the ____ property for real numbers we have $(2x^2 + 3x + 5) \cdot (4x^2 + x + 2) = (2x^2 + 3x + 5) \cdot 4x^2 + (2x^2 + 3x + 5) \cdot x + (2x^2 + 3x + 5) \cdot 2$.

- -

ANSWER:

distributive (Property A_a is also implicitly used.)

- -

Again using the distributive property we see that the preceding expression can be written

$(2x^2 \cdot 4x^2 + 3x \cdot 4x^2 + 5 \cdot 4x^2) + (2x^2 \cdot x + 3x \cdot x + 5 \cdot x) + (2x^2 \cdot 2 + 3x \cdot 2 + 5 \cdot 2)$.

Now using the properties ____ for real numbers we get $8x^4 + 12x^3 + 20x^2 + 2x^3 + 3x^2 + 5x + 4x^2 + 6x + 10$.

- -

ANSWER:

M_c and M_a (and A_a implicitly)

- -

Now we use properties ____ for real numbers to get $8x^4 + (12x^3 + 2x^3) + (20x^2 + 3x^2 + 4x^2) + (5x + 6x) + 10$.

- -

ANSWER:

A_a and A_c.

- -

5-8

Finally Property ____ for real numbers gives us $8x^4 + (12 + 2)x^3 + (20 + 3 + 4)x^2 + (5 + 6)x + 10 = 8x^4 + 14x^3 + 27x^2 + 11x + 10$.

- -

ANSWER:

D

- -

You may be more accustomed to writing the above multiplication in the following form.

$$\begin{array}{lllll}
2x^2 & + 3x & + 5 & & \\
\underline{4x^2} & \underline{+\ x} & \underline{+ 2} & & \\
8x^4 & + 12x^3 & + 20x^2 & & \\
 & 2x^3 & + 3x^2 & + 5x & \\
\hline
 & & 4x^2 & + 6x & + 10 \\
8x^4 & + 14x^3 & + 27x^2 & + 11x & + 10
\end{array}$$

In this form $8x^4 + 12x^3 + 20x^2$ represents what product?

- -

ANSWER:

$(2x^2 + 3x + 5) \cdot 4x^2$

- -

Similarly $2x^3 + 3x^2 + 5x$ represents $(2x^2 + 3x + 5) \cdot x$, and $4x^2 + 6x + 10$ represents $(2x^2 + 3x + 5) \cdot 2$. These are the products obtained above after the first application of the distributive property. In adding these products we add the coefficients of like powers of x. Here again the distributive property is used. Note that when we multiply, in general,

$(a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0) \cdot (b_mx^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0)$,

to get the coefficient of x^k we add the coefficients of all terms

$(a_r x^r) \cdot (b_s x^s) = a_r b_s x^{r+s}$ such that $r + s = k$. Thus the coefficient of x^{n+m} is ____.

ANSWER:

$a_n b_m$.

The coefficient of x^{n+m-1} is the sum of the coefficients of $(a_n x^n) \cdot (b_{m-1} x^{m-1}) = a_n b_{m-1} x^{n+m-1}$ and $(a_{n-1} x^{n-1}) \cdot (b_m x^m) = a_{n-1} b_m x^{n+m-1}$; i.e., the coefficient is ____.

ANSWER:

$a_n b_{m-1} + a_{n-1} b_m$

What is the coefficient of x^{n+m-2}?

ANSWER:

$a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m$

What is the coefficient of x^{n+m-3}?

ANSWER:

$a_n b_{m-3} + a_{n-1} b_{m-2} + a_{n-2} b_{m-1} + a_{n-3} b_m$

The above discussion of the situation when x is a real number leads us to make the following definitions for polynomials (where we now assume once more that x is a variable):

DEFINITION 13.5: Let $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ and $b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$ be polynomials. Then $(a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) + (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) =$ ____.

- -

ANSWER:

$(a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0)$.

- -

DEFINITION 13.6: Let $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ and $b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0$ be polynomials, then $(a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) \cdot (b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0) = (a_nb_m)x^{n+m}$ + (____) x^{n+m-1} + (____) $x^{n+m-2} + \ldots + (a_1b_0 + a_0b_1)x +$ ____.

- -

ANSWER:

$a_nb_{m-1} + a_{n-1}b_m$; $a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m$; a_0b_0.

- -

Although the assumption that x is a real number led us to define addition and multiplication of polynomials as in Definitions 13.5 and 13.6, when we prove things about these operations for polynomials we do not assume that x is a real number but work directly from Definitions 13.5 and 13.6.

Find the product

$(2x^4 + 2 \cdot x^3 - 3x^2 + 1 \cdot x - 1)(2x^2 - 3x + 1)$.

- -

ANSWER:

$4x^6 - 2x^5 - 10x^4 + 13x^3 - 8x^2 + 4x - 1$

- -

Find the product

$(2x^3 - 3x^2 + 2x + 1)(\sqrt{2}x^2 - \sqrt{3}x + 5)$.

- -

ANSWER:

$2\sqrt{2}x^5 + (-2\sqrt{3} - 3\sqrt{2})x^4 + (10 + 3\sqrt{3} + 2\sqrt{2})x^3 + (15 - 2\sqrt{3} + \sqrt{2})x^2 + (10 - \sqrt{3})x + 5$

- -

To prove that the commutative property holds for addition of polynomials you must show that $(a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) + (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) = (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) + (a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0)$.

Write out a proof of this and, in your proof, point out where the commutative law for addition of real numbers is used and where the definition of addition of polynomials is used.

- -

ANSWER:

(1) $(a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) + (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0)$ by definition.

(2) $(b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) + (a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) = (b_n + a_n)x^n + (b_{n-1} + a_{n-1})x^{n-1} + \ldots + (b_1 + a_1)x + (b_0 + a_0)$ by definition.

(3) $a_n + b_n = b_n + a_n$, $a_{n-1} + b_{n-1} = b_{n-1} + a_{n-1}$, $\ldots$, $a_1 + b_1 = b_1 + a_1$, $a_0 + b_0 = b_0 + a_0$ by the commutative law for addition of real numbers.

(4) Therefore $(a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0) = (b_n + a_n)x^n + (b_{n-1} + a_{n-1})x^{n-1} + \ldots + (b_1 + a_1)x + (b_0 + a_0)$.

(5) Therefore $(a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) + (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) = (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0) + (a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0)$.

The associative property for addition of polynomials can be proved similarly. The Properties A_{id} and A_{in} hold for polynomials. The additive identity is ____. The additive inverse of the polynomial $3x^6 - 4x^3 + 2x^2 - x - 1$ is ____.

ANSWER:
the zero polynomial; $-3x^6 + 4x^3 - 2x^2 + x + 1$.

The Properties M_a and M_c hold for polynomials.

$(3x^3 + x^2 + 2) + (x^2 - 3) = 3x^3 + 2x^2 - 1$.

$(2x + 1) \cdot (3x^3 + 2x^2 - 1) =$ ____

$(2x + 1) \cdot (3x^3 + x^2 + 2) + (2x + 1)(x^2 - 3) =$ ____

The above illustates the validity of Property ____ for polynomials.

ANSWER:
$6x^4 + 7x^3 + 2x^2 - 2x - 1$, $6x^4 + 7x^3 + 2x^2 - 2x - 1$, D, the distributive property.

What is the multiplicative identity for polynomials?

ANSWER:

The polynomial 1.

The fact that we have defined addition and multiplication of polynomials as if the variable x were a real number accounts for the fact that so many of the properties of addition and multiplication of real numbers carry over to these operations for polynomials.

What do you know about the degree of the product of a polynomial of degree n and a polynomial of degree m?

ANSWER:

The degree is $n + m$.

If $P(x)$ is a non-zero polynomial, what is true about the degree of $(x^2 + 2) \cdot P(x)$?

ANSWER:

The degree is greater than or equal to 2.

[Note: Your answer is incorrect if you said "greater than 2". For example, if $P(x) = 1$, then $(x^2 + 2) \cdot P(x) = x^2 + 2$, and has degree 2.]

If $Q(x)$ is a polynomial of degree 3 and $P(x)$ is a polynomial of degree 2, what is the degree of $Q(x) \cdot P(x)$?

ANSWER:

5

If $Q(x)$ is a polynomial of degree 3 and $P(x)$ is a non-zero constant polynomial, what is the degree of $Q(x) \cdot P(x)$?

ANSWER:

3

What is the degree of the constant polynomial 1?

ANSWER:

0

If $Q(x)$ is a polynomial of degree greater than 0, is there any polynomial $P(x)$ such that $Q(x) \cdot P(x) = 1$? Why?

ANSWER:

No. If $P(x)$ is the zero polynomial, then $Q(x) \cdot P(x) = 0$. If $P(x)$ is non-zero then $Q(x) \cdot P(x)$ has degree greater than 0, but 1 has degree 0.

The preceding illustrates the failure of Property ____ for polynomials.

ANSWER:

M_{in}

Which of the following polynomials have multiplicative inverses that are polynomials?

(a) $x + 1$

(b) x^3

(c) 5

(d) -3

(e) 0

- -

ANSWER:

(c) and (d).

- -

In general, what polynomials have multiplicative inverses that are polynomials?

- -

ANSWER:

The non-zero constant polynomials.

- -

If $P(x)$ and $Q(x)$ are non-zero polynomials is it possible that $P(x) \cdot Q(x) = 0$?

- -

ANSWER:

No, if $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, with $a_n \neq 0$, and $Q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$, with $b_m \neq 0$, then $a_n b_m x^{n+m}$ is a non-zero term of $P(x) \cdot Q(x)$.

- -

State the cancellation property for multiplication of polynomials.

- -

ANSWER:

If $P(x)$, $M(x)$, and $N(x)$ are polynomials such that $P(x) \cdot M(x) = P(x) \cdot N(x)$, and if $P(x) \neq 0$, then $M(x) = N(x)$.

Prove the cancellation property for multiplication of real polynomials using the fact that if $P(x)$ and $Q(x)$ are non-zero polynomials, then $P(x) \cdot Q(x) \neq 0$. (You need not list as reasons the field properties of the real numbers that you use.) If you feel that your proof is complete, skip the next item. If not, go to the suggestion below.

Suggestion: Suppose that $M(x) \neq N(x)$ and consider $P(x) \cdot M(x) - P(x) \cdot N(x)$. Can you show that this polynomial cannot be 0?

Go back to your proof. Make corrections or additions before proceeding.

PROOF: The cancellation law may be stated as follows: If $P(x) \neq 0$, then

$$P(x) \cdot M(x) = P(x) \cdot N(x) \iff M(x) = N(x)$$

Let us suppose that $M(x) \neq N(x)$ and show that this leads to a contradiction. If $M(x) \neq N(x)$, then $M(x) - N(x)$ is a non-zero polynomial. Since $P(x) \neq 0$, $P(x)[M(x) - N(x)] \neq 0$. Thus $P(x) \cdot M(x) - P(x) \cdot N(x) \neq 0$. Therefore $P(x) \cdot M(x) \neq P(x) \cdot N(x)$, a contradiction of the hypothesis.

We see that for the algebra of polynomials the field postulates ____, ____, ____, ____, ____, ____, ____, and ____, hold, while postulate ____ fails to hold.

ANSWER:

A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, D; M_{in}.

- -

What subsystem of the real numbers do you know in which all the properties A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, and D hold, in which M_{in} fails to hold, but in which the cancellation law for multiplication holds?

- -

ANSWER:

The system of integers.

- -

DEFINITION 13.7: An algebraic system which is closed under two binary operations, addition and multiplication, and in which the properties A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, D and the cancellation property for multiplication are valid is called an integral domain.

Which of the following systems are integral domains?

(a) real numbers
(b) rational numbers
(c) integers
(d) even integers
(e) positive integers
(f) polynomials

- -

ANSWER:

(a), (b), (c), (f). Remember that the cancellation law holds in any field.

- -

What basic properties of an integral domain do examples (d) and (e) of the previous item fail to have?

- -

ANSWER:

(d) Property M_{id} fails.

(e) Properties A_{id} and A_{in} fail.

- -

Two systems above which are integral domains but are not fields are the system of ____ and the system of ____.

- -

ANSWER:

integers, polynomials.

- -

DIVISION THEOREM FOR POLYNOMIALS, FACTORING

We will see that there are other striking similarities between the systems of integers and polynomials. We have seen that because Property M_{in} fails to hold in the system of integers exact division is not always possible. We did, however, introduce for the integers division with remainder. In the division theorem for integers what conditions on the remainder r were required (when a is divided by b)?

- -

ANSWER:

$0 \leq r < |b|$. Note that the answers "$0 < r < |b|$" and "$0 \leq r < b$" are not correct. Take care to state your answers precisely.

- -

State the division theorem for integers completely.

- -

ANSWER:

If each of a and b is an integer and $b \neq 0$, then there are integers q and r such that $a = q \cdot b + r$ and $0 \leq r < |b|$.

- -

There is a similar division theorem for polynomials. Let us illustrate with an example. Suppose we divide the polynomial $x^3 + 3x^2 - 2x + 1$ by $x^2 - 2x + 2$. Using long division we have

$$
\begin{array}{rl}
 & \;\; x + 5 \\
x^2 - 2x + 2 & \overline{)\,x^3 + 3x^2 - 2x + 1} \\
 & \;\; \underline{x^3 - 2x^2 + 2x} \\
 & \qquad\quad 5x^2 - 4x + 1 \\
 & \qquad\quad \underline{5x^2 - 10x + 10} \\
 & \qquad\qquad\qquad 6x - 9
\end{array}
$$

Thus we get a quotient ____ and remainder ____.

- -

ANSWER:

$x + 5$, $6x - 9$

- -

We can express the result of the above division in the following way:

$$x^3 + 3x^2 - 2x + 1 = (x + 5) \cdot (x^2 - 2x + 2) + (6x - 9)$$

In the division theorem for integers the remainder is always less than the absolute value of the divisor. In the previous example does it make sense to say that

$6x - 9 < |x^2 - 2x + 2|$? Why?

- -

ANSWER:

No. We have not assumed that polynomials are ordered. Therefore absolute value has no meaning for polynomials and it does not make sense to talk about one polynomial being less than another (unless of course the polynomials happen to be constant, i.e., real numbers).

- -

There is, however, a relationship between $6x - 9$ and $x^2 - 2x + 2$ which is important in the given division process. What is it?

- -

ANSWER:

The remainder $6x - 9$ has degree less than the degree of the divisor $x^2 - 2x + 2$.

- -

The condition $0 \leq r < |b|$ is replaced, for polynomials, by the condition that the remainder is either zero or has degree ____ the degree of the divisor.

- -

ANSWER:

less than.

- -

If the remainder is not zero its degree must be what kind of number?

- -

ANSWER:

Non-negative integer.

- -

Why cannot the condition be stated simply: the degree of the remainder is less than the degree of the divisor?

- -

ANSWER:

Because the remainder may be the zero polynomial and it has no degree.

We now give a formal statement of the division theorem for polynomials.

THEOREM 13.1: If $P(x)$ and $N(x)$ are polynomials and $N(x) \neq 0$, then there are unique polynomials $Q(x)$ and $R(x)$ such that $P(x) = Q(x) \cdot N(x) + R(x)$ where $R(x)$ is either the zero polynomial or is a non-zero polynomial whose degree is less than the degree of $N(x)$.

We call $P(x)$ the dividend, $N(x)$ the divisor, $Q(x)$ the quotient and $R(x)$ the remainder.

Why is the equation $x^3 + 3x^2 - 2x + 1 = x \cdot (x^2 - 2x + 2) + (5x^2 - 4x + 1)$ not a correct application of the division theorem (dividing $x^3 + 3x^2 - 2x + 1$ by $x^2 - 2x + 2$)?

ANSWER:

The remainder $5x^2 - 4x + 1$ has degree equal to (not less than) the degree of the divisior $x^2 - 2x + 2$.

In looking for a proof of Theorem 13.1, let us analyze the process involved in dividing $x^3 + 3x^2 - 2x + 1$ by $x^2 - 2x + 2$. The first step in the process of long division is

$$\begin{array}{rl} & x \\ x^2 - 2x + 2 & \overline{)\,x^3 + 3x^2 - 2x + 1} \\ & \underline{x^3 - 2x^2 + 2x\phantom{{}+1}} \\ & \phantom{x^3+{}}5x^2 - 4x + 1 \end{array}$$

We obtain the polynomial $x^3 - 2x^2 + 2x$ by multiplying the divisor, $x^2 - 2x + 2$, by the first term of the quotient, x.

The first term of the quotient, x, is chosen so that what will be true?

- -

ANSWER:

So that when we subtract $x \cdot (x^2 - 2x + 2)$ from the dividend $x^3 + 3x^2 - 2x + 1$ the terms of highest degree cancel. This yields a remainder, $5x^2 - 4x + 1$, of degree lower than the degree of the dividend.

- -

Thus we have

$$(x^3 + 3x^2 - 2x + 1) - x \cdot (x^2 - 2x + 2) = 5x^2 - 4x + 1,$$

or equivalently

$$x^3 + 3x^2 - 2x + 1 = x \cdot (x^2 - 2x + 2) + (5x^2 - 4x + 1).$$

The division process is not complete because ____.

- -

ANSWER:

The degree of the remainder, $5x^2 - 4x + 1$, is not less than the degree of the divisor.

- -

Hence we repeat the process using $5x^2 - 4x + 1$ as the new dividend. This process is continued until we get a remainder which ____ or ______.

- -

ANSWER:

is zero or has degree less than the degree of the divisor, $x^2 - 2x + 2$.

- -

We can indicate the division in the example shown as follows:

$x^3 + 3x^2 - 2x + 1 = x \cdot (x^2 - 2x + 2) + (5x^2 - 4x + 1),$

$5x^2 - 4x + 1 = \_\_\_\_ (x^2 - 2x + 2) + \_\_\_\_.$

ANSWER:

5; $6x - 9$.

Therefore $x^3 + 3x^2 - 2x + 1 = x \cdot (x^2 - 2x + 2) + 5 \cdot (x^2 - 2x + 2) + (6x + 9),$

$= (x + 5)(x^2 - 2x + 2) + (6x + 9).$

This is of the form given in Theorem 13.1 because $6x - 9$ has degree less than the degree of $x^2 - 2x + 2$.

The idea used in this example can be used to construct a proof of the existence part of Theorem 13.1. We observe first of all that if $P(x) = 0$ or if $P(x)$ has degree less than the degree of $N(x)$, then we can choose $Q(x) = \_\_\_\_$ and $R(x) = \_\_\_\_$ and the conditions of the theorem are fulfilled (look back at Theorem 13.1).

ANSWER:

$Q(x) = 0, \quad R(x) = P(x).$

Consider now the case where $P(x)$ has degree greater than or equal to the degree of $N(x)$. In the division process we first look for a monomial cx^k such that when we subtract $cx^k \cdot N(x)$ from $P(x)$ what happens?

ANSWER:

The terms of highest degree cancel.

Suppose $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, $a_0 \neq 0$, and $N(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$, $b_0 \neq 0$, and $n \geq m$. What can we choose for c and k so that $P(x) - cx^k \cdot N(x)$ has no term of degree n?

- -

ANSWER:

Choose $cx^k = \frac{a_0}{b_0}x^{n-m}$. Thus the term of highest degree in $cx^k \cdot N(x)$ is $\frac{a_0}{b_0}x^{n-m} \cdot b_0x^m = a_0x^n$. When we subtract $\frac{a_0}{b_0}x^{n-m} \cdot N(x)$ from $P(x)$, this term cancels.

- -

We get $P(x) = \frac{a_0}{b_0}x^{n-m} \cdot N(x) + R_1(x)$ where $R_1(x)$ is 0 or has degree less than n. We can repeat the process with $R_1(x)$ in place of $P(x)$. If the process if repeated successively, eventually we get a remainder which is 0 or which has degree less than the degree of $N(x)$.

This last step can be made rigorous by using mathematical induction. We will not do this here, nor will we prove the uniqueness part of the theorem. However, we will illustrate the process with another example.

Let $P(x) = 3x^3 - \frac{1}{2}x^2 + 3x + 5$ and $N(x) = 2x + 1$. Then

$$(3x^3 - \frac{1}{2}x^2 + 3x + 5) - \frac{3}{2}x^2(2x + 1) = -2x^2 + 3x + 5 \quad \text{or}$$

$$3x^3 - \frac{1}{2}x^2 + 3x + 5 = \frac{3}{2}x^2(2x + 1) + (-2x^2 + 3x + 5)$$

Then $-2x^2 + 3x + 5 =$ ____ $\cdot\ (2x + 1) +$ ____.

- -

ANSWER:

$-x$; $4x + 5$.

- -

Finally $4x + 5 = \_\_\_\_ \cdot (2x + 1) + \_\_\_\_.$

- -

ANSWER:

2; 3.

- -

Collecting the above we obtain

$$\begin{aligned} 3x^3 - \frac{1}{2}x^2 + 3x + 5 &= \frac{3}{2}x^2(2x + 1) + (-2x^2 + 3x + 5) \\ &= \frac{3}{2}x^2(2x + 1) + (-x)(2x + 1) + 4x + 5 \\ &= \frac{3}{2}x^2(2x + 1) + (-x)(2x + 1) + 2(2x + 1) + 3 \\ &= (\frac{3}{2}x^2 - x + 2)(2x + 1) + 3 \end{aligned}$$

Note how this division appears in the usual long division form:

$$\begin{array}{rl} & (3/2)x^2 - x + 2 \\ 2x + 1 & \overline{\big)\,3x^3 - (1/2)x^2 + 3x + 5} \\ & \underline{3x^3 + (3/2)x^2} \\ & \qquad -2x^2 + 3x + 5 \\ & \qquad \underline{-2x^2 - x \qquad} \\ & \qquad\qquad\qquad 4x + 5 \\ & \qquad\qquad\qquad \underline{4x + 2} \\ & \qquad\qquad\qquad\qquad 3 \end{array}$$

In the equation $P(x) = Q(x) \cdot N(x) + R(x)$, obtained from the division theorem if $R(x)$ happens to be the zero polynomial, then $P(x)$ is exactly divisible by $N(x)$. We say that $N(x)$ and $Q(x)$ are factors of $P(x)$, for we have $P(x) = Q(x) \cdot N(x)$. We will see that factoring of polynomials is similar, in many respects, to factoring of integers, which we have already discussed.

In studying the factorization of integers we saw that the integers 1 and -1 are factors of every integer. This is due to the fact that 1 and -1 have ____ which are integers.

- -

ANSWER:

multiplicative inverses.

Because 1 and -1 have multiplicative inverses which are integers we call them ____ of the system of integers.

ANSWER:

units.

DEFINITION 13.8: In any integral domain the elements which have multiplicative inverses in the integral domain are called units.

Field Property ____ tells us that every non-zero element of a field has a multiplicative inverse.

ANSWER:

M_{in}.

What are the units of a field?

ANSWER:

All the non-zero elements of the field.

In the system of polynomials the only elements which have multiplicative inverses are ____.

ANSWER:

The non-zero constant polynomials.

- -

The non-zero constant polynomials are the ____ of the system of polynomials.

- -

ANSWER:

units.

- -

In the integral domain of polynomials, a unit is a factor of every polynomial. Thus we could write $x - 2 = 2 \cdot (x/2 - 1)$ or $x - 2 = 1/3 \cdot (3x - 6)$.

The first example illustrates that 2 is a factor of $x - 2$ and the second example illustrates that $1/3$ is a factor of $x - 2$. In fact, if c is a unit, i.e., a non-zero constant polynomial, and $P(x)$ is any polynomial we can write $P(x) = c \cdot [1/c\ P(x)]$

Since c is a polynomial and $1/c\ P(x)$ is a polynomial, c is a factor of $P(x)$. In discussing factorization of polynomials we will be particularly interested in factorizations in which the factors are not units.

What is true about the degree of a non-zero polynomial if it is not a unit?

- -

ANSWER:

The degree is greater than zero.

- -

Which of the following polynomials are units?

(a) $\sqrt{2}$

(b) x

(c) $2x^2 + 3$

(d) 0

(e) -1

- -

ANSWER:

(a) and (e). The polynomials x, $2x^2 + 3$, and 0 do not have multiplicative inverses which are polynomials. $\sqrt{2}$ has inverse $1/\sqrt{2}$ and -1 has inverse -1.

- -

DEFINITION 13.9: A non-zero polynomial is said to be factorable if it can be written as a product of factors which are not units. (Some books use the term reducible instead of factorable.)

What is true about the degree of any factorable polynomial? Why?

- -

ANSWER

The degree is greater than one, because the degree of any factor which is not a unit must be at least one.

- -

Is a constant polynomial factorable?

- -

ANSWER:

No, it cannot be written as a product of non-constant polynomials.

- -

DEFINITION 13.10: A polynomial is called irreducible if it is non-constant and not factorable.

The irreducible polynomials are the analogues of the ____ in the system of integers.

- -

ANSWER:

prime numbers.

The non-zero constant polynomials are the analogues of the integers 1 and -1 because the non-zero constant polynomials are the ____ of the system of polynomials while 1 and -1 are the ____ of the system of integers.

ANSWER:

units; units.

Composite integers are the analogues of the ____ polynomials.

ANSWER:

factorable.

In the system of integers we know that: 1 and -1 are neither prime nor composite. The analogue of this statement for polynomials is: the ____ polynomials are neither ____ nor ____.

ANSWER:

non-zero constant; irreducible; factorable.

Is the polynomial $4x - 4$ factorable?

ANSWER:

No. It cannot be written as a product of factors which are not units. In the factorization $4(x - 1)$, the factor 4 is a unit.

- -

Is the polynomial 5 irreducible?

- -

ANSWER:

No. Irreducible polynomials are non-constant, by definition.

- -

The set of integers can be separated into four subsets, no two of which have any elements in common. Those are:

(1) the set $\{0\}$,
(2) the set of units $\{1, -1\}$,
(3) the set of primes, and
(4) the set of composites.

The set of polynomials can similarly be separated into four subsets no two of which have any elements in common. These are:

(1) _____,
(2) ____,
(3) ____,
(4) ____.

- -

ANSWER:

(1) The set $\{0\}$.
(2) The set of units - the non-zero constant polynomials.
(3) The set of irreducible polynomials.
(4) The set of factorable polynomials.

- -

Indicate to which of these four sets each of the following real polynomials belongs by placing one of the numbers (1), (2), (3), or (4) in each of the blank spaces.

(a) $x^2 - 4$ ____

(b) -3 ____

(c) $2x + 1$ ____

(d) 0 ____

(e) $3x - 3$ ____

- -

ANSWER:

(a) 4, (b) 2, (c) 3, (d) 1, (e) 3.

- -

In order to be irreducible a polynomial must have degree greater than ____ and cannot be written as a product of polynomials each of which has degree greater than ____.

- -

ANSWER:

zero; zero.

- -

Which of the following polynomials are factorable and which are irreducible?

(a) $2x + 2$

(b) $x^2 - 1$

(c) $2x + 3$

(d) 3

- -

ANSWER:

(a) irreducible

(b) factorable

(c) irreducible

(d) constant, therefore neither factorable nor irreducible

- -

If a non-constant polynomial $P(x)$ is not irreducible, then it can be factored, $P(x) = Q(x) \cdot N(x)$, in such a way that $Q(x)$ and $N(x)$ are non-constant and have degrees ____ than the degree of $P(x)$.

- -

ANSWER:

less.

- -

Consider the polynomial $P(x) = 2x^2 - 1$, $P(x)$ can be factored as follows:

$P(x) = 2(x - \sqrt{1/2})(x + \sqrt{1/2})$.

In this factorization, 2 is a unit and $x - \sqrt{1/2}$ and $x + \sqrt{1/2}$ are ____ polynomials with leading coefficient ____.

- -

ANSWER:

irreducible; one.

- -

For integers we learned that each non-zero integer n which is not a unit has a unique standard factorization of the form $n = c \cdot p_1 \cdot p_2 \cdots p_k$ where c is a unit and each of $p_1, p_2, \ldots, p_k$ are positive primes. Can you guess an analogue of this statement for polynomials? (Hint: Take, as analogue of positive prime, irreducible polynomial whose leading coefficient is one. You must also decide what is the analogue of "non-zero integer n which is not a unit.") Write your answer as a complete statement paralleling the statement given for integers.

- -

ANSWER:

THEOREM 13.2: Each non-constant polynomial $P(x)$ has a unique standard factorization of the form $P(x) = c \cdot P_1(x) \cdot P_2(x) \ldots P_k(x)$, where c is a unit and each of $P_1(x), P_2(x), \ldots, P_k(x)$, is an irreducible polynomial whose leading coefficient is one.

- -

DEFINITION 13.11: A polynomial whose leading coefficient is one is called a monic polynomial.

In Theorem 13.2 the polynomials $P_1(x), P_2(x), \ldots, P_k(x)$ are irreducible monic polynomials.

Find the standard factorization for each of the following polynomials:

(i) $2x^2 + 4x + 2 =$ ____

(ii) $x^2/3 - 1 =$ ____

(iii) $-x^2 =$ ____

(iv) -4

(v) $x^3 + 1 =$ ____

- -

ANSWER:

(i) $2(x + 1)(x + 1)$

(ii) $1/3(x + \sqrt{3})(x - \sqrt{3})$

(iii) $(-1)(x)(x)$

(iv) -4 is a unit; therefore it has no standard factorization

(v) $(1)(x + 1)(x^2 - x + 1)$

- -

In trying to prove Theorem 13.2 let us first see if we can prove the following weaker statement:

(A) Each non-constant polynomial $P(x)$ can be written in the form

$P(x) = Q_1(x)\, Q_2(x) \ldots Q_\ell(x), \quad \ell \geq 1$

where each of $Q_1(x)$, $Q_2(x)$, ... $Q_\ell(x)$ is an irreducible polynomial.

If $P(x)$ is itself irreducible then statement (A) is trivially true by taking $Q_1(x) = P(x)$ and $\ell = 1$. If $P(x)$ is not irreducible what must be true?

- -

ANSWER:

$P(x)$ is factorable; i.e., $P(x) = M(x) \cdot N(x)$ where $M(x)$ and $N(x)$ have degrees less than the degree of $P(x)$.

- -

If $P(x) = M(x) \cdot N(x)$ then either $M(x)$ and $N(x)$ are irreducible or can be factored as products of polynomials of still lower degree. This process can be continued until $P(x)$ is factored as a product of irreducible factors.

The argument just outlined can be made rigorous by using mathematical induction. The idea is to suppose that statement (A) is not true. Then there will be some polynomial $P(x)$ of least degree for which it fails. State why this is true and try to give a complete proof of statement (A).

If you feel you have given a complete proof of statement (A), go to page 528. If not go to the next item below.

- -

Suggestion: If we assume that statement (A) is false then there is a non-empty set S of natural numbers consisting of all those numbers which are degrees of polynomials for which statement (A) fails. The well-ordering property of the natural numbers tells us there is a least number k in S. Let $P(x)$ be a polynomial of degree k for which statement (A) fails. Then $P(x)$ is not irreducible.

Go back to your proof. Make additions or corrections. Then if you think you have given a complete proof, go to $\boxed{\dagger\dagger}$ on page 528. If not go to the next item.

Suggestion: We can write $P(x) = M(x) \cdot N(x)$ where $M(x)$ and $N(x)$ have degrees less than k. Since k is the least degree of a polynomial for which statement (A) fails we conclude that statement (A) holds for $M(x)$ and $N(x)$.

Go back to your proof. Make additions or corrections, then go on to the next item.

Your proof may differ in some respects from the one given and still be correct. However you should check carefully the following things:

(1) Did you use the well-ordering principle as a reason for the existence of a polynomial $P(x)$ of least degree for which statement (A) fails?

(2) Did you show explicitly how we arrive at a contradiction of the assumption that statement (A) is false?

Go back to your proof. Complete it if you have not done so. Then check your proof with the one given below.

$\boxed{++}$ PROOF: Suppose statement (A) is not true. Let S be the set of natural numbers which are degrees of polynomials which fail to have the property given in statement (A). Then S has a least member k, by the well-ordering property. Let $P(x)$ be a polynomial of degree k which fails to have the property given in statement (A). $P(x)$ is not irreducible. So $P(x) = M(x) \cdot N(x)$ where $M(x)$ and $N(x)$ have degrees less than k. Therefore $M(x)$ and $N(x)$ can be written in the forms:

$M(x) = Q_1(x)\, Q_2(x) \ldots Q_r(x)$, $r \geq 1$, and $N(x) = Q_1'(x)\, Q_2'(x) \ldots Q_s'(x)$, $s \geq 1$, where each of $Q_1(x), Q_2(x), \ldots, Q_r(x), Q_1'(x), Q_2'(x), \ldots, Q_s'(x)$ is irreducible. But then

$$P(x) = Q_1(x)\, Q_2(x) \ldots Q_r(x)\, Q_1'(x)\, Q_2'(x) \ldots Q_s'(x),$$

which is of the form given in statement (A). Therefore $P(x)$ has the property given in statement (A). This is a contradiction, because $P(x)$ was chosen above not to have that property. Therefore our assumption that statement (A) is false leads to a contradiction. So statement (A) is true.

Having proved statement (A), let us continue the proof of Theorem 13.2.

If $Q_i(x)$ is a polynomial with leading coefficient a_i, what is the leading coefficient of $1/a_i\ Q_i(x)$?

ANSWER:

The leading coefficient is one; i.e., $1/a_i\ Q_i(x)$ is monic.

Consider the factorization:

$P(x) = (2x^2 + 3)(3x - 1)(-2x + 2)$.

Write $P(x)$ in the form

$P(x) = cP_1(x)\ P_2(x)\ P_3(x)$,

where c is a unit, and $P_1(x)$, $P_2(x)$, $P_3(x)$ are monic irreducible polynomials.

ANSWER:

$P(x) = -12(x^2 + 3/2)(x - 1/3)(x - 1)$.

Suppose $P(x) = Q_1(x)\ Q_2(x) \ldots Q_k(x)$, where $Q_1(x)$ has leading coefficient a_1, $Q_2(x)$ has leading coefficient a_2, etc. What can we choose for c, $P_1(x)$, $P_2(x)$, ... $P_k(x)$ so that c is a unit, each $P_i(x)$ is a monic irreducible polynomial, and $P(x) = cP_1(x)$ $P_2(x) \ldots P_k(x)$?

ANSWER:

Choose $c = a_1 \cdot a_2 \ldots a_k$, $P_1(x) = 1/a_1\, Q_1(x)$, $P_2(x) = 1/a_2\, Q_2(x)$, ... $P_k(x) = 1/a_k\, Q_k(x)$.

- -

We have therefore shown that every non-constant polynomial $P(x)$ has a factorization of the form $P(x) = cP_1(x) \cdot P_2(x) \ldots P_k(x)$, where c is a unit and each of $P_1(x)$, $P_2(x)$, ..., $P_k(x)$ is a monic irreducible polynomial.

Does this complete the proof of Theorem 13.2? Explain.

- -

ANSWER:

No. To complete the proof we must show that a factorization of a non-constant polynomial in the required form is unique.

- -

Show that the factorization of a polynomial in the form given by statement (A) is not unique by showing two factorizations of the polynomial $x^2 - 1$ as a product of irreducible factors.

- -

ANSWER:

For example, $x^2 - 1 = (x + 1)(x - 1)$ and $x^2 - 1 = (2x + 2)(1/2\, x - 1/2)$. This does not contradict Theorem 13.2 because in the second factorization the factors are not monic.

- -

We will not prove the uniqueness part of Theorem 13.2 here. [A proof may be found in Birkhoff and MacLane: A Survey of Modern Algebra, New York: MacMillan, 1960, pp. 76-77.]

REMAINDER AND FACTOR THEOREMS

Using the division theorem we can prove an important result for polynomials. First, we illustrate the result with an example. Consider the polynomial $x^3 - 3x^2 + 4x + 2$. Let us divide this polynomial by $x - 2$ to get a quotient and remainder, as in the division theorem. Since the divisor $x - 2$ has degree one we know that the remainder must be a ____ polynomial.

- -

ANSWER:

constant

- -

You may check, using long division or otherwise, that we have

$x^3 - 3x^2 + 4x + 2 = (x^2 - x + 2) \cdot (x - 2) + 6$;

i.e., the quotient is $x^2 - x + 2$ and the remainder is 6.

Now let us substitute 2 in place of x in the polynomial

$x^3 - 3x^2 + 4x + 2$. We obtain $2^3 - 3 \cdot (2^2) + 4 \cdot 2 + 2 = 6$

The remainder that we get upon dividing $x^3 - 3x^2 + 4x + 2$ by $x - 2$ is just the number that we get when we substitute 2 in place of x in the dividend. We shall see that this is not a coincidence.

As a matter of notation, if $P(x)$ is a polynomial and c is a real number, then $P(c)$ will denote the number that we obtain if we substitute c in place of x in the polynomial $P(x)$. There is a way of looking at this which makes it consistent with the functional notation that we have used previously. We know that each polynomial $P(x)$ determines a polynomial function. Call this function P. Then $P(c)$, as defined above, is precisely the same as it was defined using functional notation; i.e., $P(c)$ is the number which is paired with c by the function P.

Now, let $P(x)$ be a polynomial and let c be a real number. By the division theorem, applied to $P(x)$ and $x - c$, there are polynomials $Q(x)$ and $R(x)$ such that $P(x) = Q(x) \cdot (x - c) + R(x)$, where, in this case, $R(x)$ must be ____.

- -

ANSWER:
a constant polynomial, i.e., a real number.

- -

We emphasize that $R(x)$ is a constant by writing $R(x) = r$. If we substitute c in place of x in that foregoing equation, we obtain

$P(c) =$ ____.

- -

ANSWER:
$P(c) = Q(c) \cdot (c - c) + r = 0 + r = r.$

- -

We have proved the following theorem:

THEOREM 13.3: (Remainder Theorem) If $P(x)$ is a (real) polynomial and c is a real number, then the remainder r upon division of $P(x)$ by $x - c$ is a constant polynomial, and $r = P(c)$.

Let $P(x) = x^{20} - 3x^{14} - 7x^3 + 2$. If we divide $P(x)$ by $x - 1$, the Remainder Theorem tells us that the remainder is $P(1) = 1^{20} - 3(1)^{14} - 7(1)^3 + 2 = -7$. Note that the Remainder Theorem does not tell us what the quotient is.

Without actually dividing find the remainder obtained in each of the following divisions.

(i) $x^{10} - 3x^5 + x^3 - 2$ by $x + 1$.
(ii) $x^8 + 3x^4 + 1$ by $x - \sqrt[4]{3}$.

- -

ANSWER:

(i) 1, (ii) 19.

- -

DEFINITION 13.12: If $P(x)$ is a polynomial and c is a real number such that $P(c) = 0$, then c is called a root of the polynomial $P(x)$.

From the Remainder Theorem we see that a real number c is a root of a polynomial $P(x)$ if and only if ____.

- -

ANSWER:

the remainder upon division of $P(x)$ by $x - c$ is zero.

- -

This gives us the following theorem.

THEOREM 13.4: (Factor Theorem) If $P(x)$ is a non-constant (real) polynomial and c is a real number, then c is a root of $P(x)$ if and only if $x - c$ is a ____ of $P(x)$.

- -

ANSWER:

factor

- -

The Factor Theorem gives us one answer to the question: Why do we study factoring in algebra? For example, if we know that the polynomial $P(x) = x^3 + x^2 - 2x - 2$ can be factored thusly: $P(x) = (x - \sqrt{2})(x + \sqrt{2})(x + 1)$, we know immediately that the roots of $P(x)$ are ____.

- -

ANSWER:

$\sqrt{2}$, $-\sqrt{2}$, and -1.

- -

The Factor Theorem can be used as an aid in factoring a polynomial. For example if $P(x) = x^5 - 32 = x^5 - 2^5$, it is clear that ____ is a root of $P(x)$. Hence we know that ____ is a factor of $P(x)$.

- -

ANSWER:

2, $x - 2$. In fact $x^5 - 32 = (x - 2)(x^4 + 2x^3 + 4x^2 + 8x + 16)$.

- -

Using the Factor Theorem find a factor of degree one of each of the following polynomials:

(a) $x^4 + x^3 + x^2 - 1$

(b) $x^{10} - 3^{10}$

(c) $x^9 + 2^9$

- -

ANSWER:

(a) $x + 1$

(b) $x - 3$ or $x + 3$

(c) $x + 2$.

- -

If n is an odd positive integer and c is a real number then $(-c)^n$ = ____.

- -

ANSWER:

$-c^n$.

- -

Therefore $-c$ is a root of the polynomial ____.

- -

ANSWER:
$x^n + c^n$.

- -

This proves that if n is an odd positive integer and c is a real number, then ____ is a factor of $x^n + c^n$.

- -

ANSWER:
$x + c$.

- -

If n is an even positive integer then $(-c)^n + c^n =$ ____.

- -

ANSWER:
$2c^n$

- -

We conclude that if n is an even positive integer and c is a real number then $x + c$ is not a factor of $x^n + c^n$ unless ____.

- -

ANSWER:
$c = 0$.

- -

Use the Factor Theorem to prove that if n is an odd positive integer then $x + 1$ is a factor of $x^n + x^{n-1} + x^{n-2} + \ldots + x + 1$.

- -

ANSWER:
If n is odd, then n, $n - 2$, $n - 4$, ..., 1 are odd, while $n - 1$, $n - 3$, $n - 5$, ..., 2 are even. So

$(-1)^n + (-1)^{n-1} + (-1)^{n-2} + \ldots + (-1) + 1 = -1 + 1 - 1 + 1 \ldots - 1 + 1 = 0$.

Therefore -1 is a root of $x^n + x^{n-1} + x^{n-2} + \dots + x + 1$ and by the Factor Theorem, this polynomial has $x - (-1) = x + 1$ as a factor.

- -

If n is an even positive integer what is the remainder obtained when we divide $x^n + x^{n-1} + x^{n-2} + \dots + x + 1$ by $x + 1$?

- -

ANSWER:

The remainder is $(-1)^n + (-1)^{n-1} + (-1)^{n-2} + \dots + (-1) + 1 =$ $1 - 1 + 1 - 1 + \dots - 1 + 1 = 1$.

- -

Therefore $x + 1$ is not a factor of $x^n + x^{n-1} + x^{n-2} + \dots + x + 1$ if n is an even positive integer.

Is $x - 1$ a factor of $x^n + x^{n-1} + \dots + x + 1$ if n is an even positive integer? ____, if n is an odd positive integer? ____.

- -

ANSWER:

no, no.

- -

Suppose c is a root of a polynomial $P(x)$. By the Factor Theorem $x - c$ is a factor of $P(x)$; i.e., $P(x) = (x - c)\,Q(x)$. If $P(x)$ has degree n what is the degree of $Q(x)$?

- -

ANSWER:

$n - 1$.

- -

How are the roots of $P(x)$ and of $Q(x)$ related?

- -

ANSWER:

Every root of $Q(x)$ is a root of $P(x)$. Every root of $P(x)$ different from c is a root of $Q(x)$.

- -

Prove that if $d \neq c$ and d is a root of $P(x)$ then d is a root of $Q(x)$.

- -

ANSWER:

If d is a root of $P(x)$, then $P(d) = 0$. Hence $(d - c)\, Q(d) = 0$. If $d \neq c$, then $d - c \neq 0$ and so $Q(d) = 0$; i.e., d is a root of $Q(x)$.

- -

If $P(x) = (x - c)\, Q(x)$ and $Q(x)$ has k (distinct) roots, how many roots does $P(x)$ have?

- -

ANSWER:

Either k roots or $k + 1$ roots. If c is a root of $Q(x)$ then $P(x)$ has the same roots as $Q(x)$. If c is not a root of $Q(x)$ then $P(x)$ has one more root than $Q(x)$.

- -

Let $P(x)$ be a polynomial of degree 1, say $P(x) = ax + b$, $a \neq 0$. What are the roots of $P(x)$?

- -

ANSWER:

There is only one root, $-b/a$.

- -

The following important theorem can be proved using the Factor Theorem.

THEOREM 13.5: If $P(x)$ is a polynomial of degree $n > 0$, then $P(x)$ has at most n roots.

In order to prove Theorem 13.5 by induction, it is sufficient to show two things:

(1) The theorem is true for polynomials of degree $n = 1$, and

(2) ____.

- -

ANSWER:

If the theorem is true for polynomials of degree k (some positive integer), then it is also true for polynomials of degree $k + 1$.

- -

We have already shown that the theorem is true for polynomials of degree 1. Assume that it is true for polynomials of degree $k \geq 1$ and let $P(x)$ be a polynomial of degree $k + 1$. Complete the proof.

- -

ANSWER:

If c is a root of $P(x)$ then, by the Factor Theorem, $P(x) = (x - c) \cdot Q(x)$. $Q(x)$ has degree k. By the assumption, $Q(x)$ has at most k roots. $P(x)$ has either the same roots as $Q(x)$ or one root more than $Q(x)$. So $P(x)$ has at most $k + 1$ roots.

- -

RATIONAL AND COMPLEX POLYNOMIALS

Thus far in our discussion of polynomials, the basic underlying system has been that of the real numbers. We have assumed that the coefficients of a polynomial are real numbers. This assumption, however, is not necessary. We can carry out a similar discussion for polynomials whose coefficients are restricted to be rational numbers; or we can allow the coefficients to be arbitrary complex numbers. More generally, we can develop the preceding notions for polynomials where the basic underlying system is taken to be any field.

Since the rational numbers are themselves real numbers and the real numbers are complex numbers, the polynomials with rational coefficients form a subsystem of the system of polynomials with real coefficients, and each of these is a subsystem of the system of polynomials with complex coefficients. It is often very important that the system with which we are working be clearly specified. For example, consider the question: Is the polynomial $x^2 - 2$ factorable?

If we are working with the system of real polynomials, the answer is ____; but if we are working with the system of rational polynomials, the answer is ____.

ANSWER:

yes;

no.

Thus $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, and $x - \sqrt{2}$ and $x + \sqrt{2}$ are real polynomials but are not rational polynomials. We say that $x^2 - 2$ is factorable over the real numbers but is not factorable over the rational numbers. When students are given problems in factoring of polynomials it should always be made clear from what system the coefficients may be taken.

Is $x^2 + 1$ factorable over the rational numbers? ____, the real numbers? ____ the complex numbers? ____.

ANSWER:

no; no; yes.

Factor the polynomial $x^4 - 4$ as a product of irreducible factors

(a) over the rational numbers

(b) over the real numbers

(c) over the complex numbers

ANSWER:

(a) $(x^2 - 2) \cdot (x^2 + 2)$

(b) $(x - \sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 2)$

(c) $(x - \sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x - \sqrt{2}i) \cdot (x + \sqrt{2}i)$.

When we say that a polynomial is irreducible we must specify the system with which we are working. Thus we say that $x^2 - 2$ is irreducible over the ____ but is not irreducible over the ____.

ANSWER:

rational numbers; real numbers, or complex numbers.

Consider the polynomial $6x^2 - 7x + 2$. We can easily find its roots by factoring or by using the quadratic formula. However, let us look at another way of finding information about any possible rational roots of the polynomial. Suppose u/v is a non-zero rational root of the polynomial written as a fraction of integers in lowest terms. Then

$$6(u/v)^2 - 7(u/v) + 2 = 0$$

$$6u^2/v^2 - 7u/v + 2 = 0$$

$$6u^2 - 7uv + 2v^2 = 0$$

$$6u^2 - 7uv = -2v^2$$

$$-u(6u^2 - 7v) = +2v^2$$

How can we conclude that u is a divisor of 2?

ANSWER:

u and v are relatively prime because u/v is in lowest terms. Therefore u and v^2 are relatively prime. Since u is a factor of $2v^2$, u must be a factor of 2.

What are the possible values for u?

ANSWER:

1, -1, 2, -2.

From $6u^2 - 7uv + 2v^2 = 0$ we can also write

$6u^2 = v(7u - 2v)$.

In a manner similar to the above we conclude that v is a factor of ____.

ANSWER:

6.

Recall that if u/v is in lowest terms then v is positive. What are the possible values for v?

ANSWER:

1, 2, 3, and 6.

- -

From the above information we can conclude that the only possible rational roots of the polynomial $6x^2 - 7x + 2$ are ____.

- -

ANSWER:

1, -1, 1/2, -1/2, 1/3, -1/3, 1/6, -1/6, 2, -2, 2/3, -2/3.

If we substitute each of these numbers in place of x in the polynomial we find that the roots are 2/3 and 1/2.

- -

Consider the following problem: Find all rational roots, if there are any, of the polynomial $3x^5 - 2x^4 - 3x^2 + x - 2$. If u/v is a rational root written as fraction in lowest terms then

$$3(u/v)^5 - 2(u/v)^4 - 3(u/v)^2 + u/v - 2 = 0$$

$$3u^5 - 2u^4v - 3u^2v^3 + uv^4 - 2v^5 = 0$$

$$u(3u^4 - 2u^3v - 3uv^3 + v^4) = 2v^5$$

As in the previous example we see that u is a divisor of 2. Hence the only possible values for u are ____.

- -

ANSWER:

1, -1, 2, -2.

- -

What are the possible values for v?

- -

ANSWER:

1 and 3. Since $3u^5 = v(2u^4 + 3u^2v^2 - uv^3 + 2v^4)$, v is a divisor of 3. v is positive because u/v is in lowest terms. Therefore v must be either 1 or 3.

- -

What are the only possible rational roots of $3x^5 - 2x^4 - 3x^2 + x - 2$?

- -

ANSWER:

1, -1, 2, -2, 1/3, -1/3, 2/3, -2/3.

Substitution of these numbers in place of x shows that 2/3 is the only rational root.

- -

Assume that $P(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ is a polynomial with integer coefficients and that $a_n \neq 0$, $a_0 \neq 0$. Suppose u/v is a rational root of $P(x)$ written as a fraction in lowest terms. Then

$$a_n(u/v)^n + a_{n-1}(u/v)^{n-1} + \ldots + a_1(u/v) + a_0 = 0$$

$$a_nu^n + a_{n-1}u^{n-1}v + \ldots + a_1uv^{n-1} + a_0v^n = 0$$

$$-u(a_nu^{n-1} + a_{n-1}u^{n-2}v + \ldots + a_1v^{n-1}) = a_0v^n$$

Reasoning as in the previous examples we see that u is a factor of a_0. Show that v is a factor of a_n.

- -

ANSWER:

From $a_nu^n + a_{n-1}u^{n-1}v + \ldots + a_1uv^{n-1} + a_0v^n = 0$ we get

$$a_nu^n = -v(a_{n-1}u^{n-1} + \ldots + a_1uv^{n-2} + a_0v^{n-1}).$$

Since u/v is in lowest terms, u and v are relatively prime.

Hence u^n and v are relatively prime. Therefore v is a divisor of a_n.

We have proved the following theorem.

THEOREM 13.6: If $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a polynomial with integer coefficients, $a_n \neq 0$, $a_0 \neq 0$, and if u/v is a rational root of $P(x)$ written as fraction in lowest terms, then u is a divisor of a_0 and v is a divisor of a_n.

Find all the rational roots, if any, of the polynomial $3x^5 + x^4 - 3x^2 + 2x + 1$.

ANSWER:

$-1/3$. If u/v is a rational root written as a fraction in lowest terms then u is a divisor of 1 and v is a divisor of 3. Hence the only possible rational roots are $1, -1, 1/3, -1/3$. Substitution of these numbers in place of x shows that $-1/3$ is the only rational root.

Show that the polynomial $x^{37} - 2x^{24} + 3x^{16} - x + 1$ has no rational roots.

ANSWER:

If u/v is a rational root written as a fraction in lowest terms then u is a divisor of 1 and v is a divisor of 1. Hence the only possible rational roots are 1 and -1. Substitution of each of these in place of x shows that neither is a root.

Give an example of a non-constant real polynomial which has no real roots.

- -

ANSWER:

e.g., $x^2 + 1$. Of course there are many other correct answers.

- -

Every non-constant real polynomial, and in fact every non-constant complex polynomial, does have a root in the field of complex numbers. This is a consequence of the following theorem.

THEOREM 13.7: (Fundamental Theorem of Algebra) If $P(x)$ is a non-constant polynomial with complex number coefficients then there is a complex number c such that $P(c) = 0$; i.e., $P(x)$ has a root in the field of complex numbers.

The proof of this theorem is too difficult to be given here.*

If $P(x)$ is a non-constant polynomial with complex number coefficients then the Fundamental Theorem of Algebra tells us that $P(x)$ has a root c. The Factor Theorem tells us that $P(x)$ has ____ as a factor.

- -

ANSWER:

$x - c$.

- -

Show that $x - (1 + i)$ is a factor of the polynomial $x^3 + (1 - i)x - 2i$.

- -

---

* A proof may be found in Hille: Analytic Function Theory, Vol I, New York: Ginn, 1959, pp. 207-208.

ANSWER:

$(1 + i)^3 + (1 - i)(1 + i) - 2i = 1 + 3i + 3i^2 + i^3 + 1 - i^2 - 2i =$
$1 + 3i - 3 - i + 1 + 1 - 2i = 0.$

Therefore $1 + i$ is a root of $x^3 + (1 - i)x - 2i$ and, by the Factor Theorem, $x - (1 + i)$ is a factor.

- -

Is $x - 2$ a factor of the complex polynomial $x^4 - ix^2 + (2 + i)x - 20 + 2i$?

- -

ANSWER:

Yes; $2^4 - i(2)^2 + (2 + i) \cdot 2 - 20 + 2i$
$= 16 - 4i + 4 + 2i - 20 + 2i = 0.$

2 is a root and $x - 2$ is a factor.

- -

If $P(x)$ is irreducible over the field of complex numbers what is true about its degree?

- -

ANSWER:

It has degree 1. If $P(x)$ has degree greater than 1, then $P(x) = (x - c)\,Q(x)$ where c is a root of $P(x)$ and $Q(x)$ is a non-constant polynomial.

- -

We see that a complex polynomial $P(x)$ of degree $n > 1$ is always factorable over the complex numbers as a product:

$P(x) = P_1(x) \cdot P_2(x) \ldots P_n(x),$

where the degree of each of $P_1(x)$, $P_2(x)$, ..., $P_n(x)$ is ____.

- -

ANSWER:

one.

What are the (complex) roots of $x^2 - 4x + 5$?

ANSWER:

$2 + i$ and $2 - i$.

Find factors of $x^2 - 4x + 5$ which are irreducible over the complex numbers.

ANSWER:

$x - (2 + i)$ and $x - (2 - i)$.

The complex conjugate of $2 + i$ is ____.

ANSWER:

$2 - i$.

Assume that $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ is a real polynomial and that c is a root of $P(x)$ from the field of complex numbers. Then $P(c) = 0$. Let $\bar{c}$ be the complex conjugate of c.

$P(\bar{c})$ = ____.

ANSWER:

$a_n(\bar{c})^n + a_{n-1}(\bar{c})^{n-1} + \dots + a_1\bar{c} + a_0$.

Theorem 11.5 permits us to rewrite this as follows:

$P(\bar{c})$ = ____.

- -

ANSWER:

$a_n\overline{c^n} + a_{n-1}\overline{c^{n-1}} + \ldots + a_1\bar{c} + a_0$.

- -

$a_n = \overline{a_n}$, $a_{n-1} = \overline{a_{n-1}}$, ..., $a_1 = \overline{a_1}$, $a_0 = \overline{a_0}$. Why?

- -

ANSWER:

a_n, a_{n-1}, ..., a_1, a_0 are real numbers.

- -

Therefore $P(\bar{c}) = \overline{a_n}\,\overline{c^n} + \overline{a_{n-1}}\,\overline{c^{n-1}} + \ldots + \overline{a_1}\,\bar{c} + \overline{a_0}$.

Using Theorem 11.4 we can rewrite this:

$P(\bar{c})$ = ____.

- -

ANSWER:

$P(\bar{c}) = \overline{a_n c^n} + \overline{a_{n-1}c^{n-1}} + \ldots + \overline{a_1 c} + \overline{a_0}$.

- -

Finally, a repeated use of Theorem 11.3 permits us to write

$P(\bar{c}) = \overline{a_n c^n + a_{n-1}c^{n-1} + \ldots + a_1 c + a_0} = \overline{P(c)}$

What is $\overline{P(c)}$?

- -

ANSWER:

$\overline{P(c)} = \overline{0} = 0.$

- -

Therefore $P(\overline{c}) = 0$ and $\overline{c}$ is a root of $P(x)$. We state this result as

THEOREM 13.8: If $P(x)$ is a real polynomial and c is a complex number which is a root of $P(x)$, then $\overline{c}$ is also a root of $P(x)$.

If you know that $\sqrt{2} - 3i$ is a root of a real polynomial $P(x)$, what is a second root?

- -

ANSWER:

$\sqrt{2} + 3i.$

- -

If c is a real root of a real polynomial $P(x)$, then $\overline{c} = c$ and Theorem 13.8 has no content. However, if c is not real then $c \neq \overline{c}$. In this case the Factor Theorem tells us that $P(x)$ has the factors ____ and ____.

- -

ANSWER:

$x - c$

$x - \overline{c}.$

- -

Therefore $P(x)$ has as factor

$(x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}.$

What is true about the numbers $c + \overline{c}$ and $c \cdot \overline{c}$?

- -

ANSWER:

They are real numbers.

- -

Let P(x) be a real polynomial of degree greater than two. Theorem 13.7 tells us that ____.

- -

ANSWER:

P(x) has a root in the field of complex numbers.

- -

Let c be a root of P(x). If c is a real number then

$P(x) = (x - c)\,Q(x).$

If c is not a real number, then

$P(x) = (x^2 - (c + \bar{c})x + c \cdot \bar{c})\,Q(x).$

In either case, Q(x) is a real polynomial whose degree is greater than ____.

- -

ANSWER:

0.

- -

What can we conclude about the degree of a real polynomial which is irreducible over the field of real numbers?

- -

ANSWER:

The degree must be 1 or 2.

- -

Every real polynomial with degree greater than 2 is not ____ over the real numbers.

- -

ANSWER:

irreducible.

- -

A real polynomial $P(x)$ of degree $n > 2$ is always factorable as a product

$$P(x) = P_1(x)\, P_2(x) \ldots P_k(x)$$

of $k (\leq n)$ factors where each of $P_1(x)$, $P_2(x)$, ..., $P_k(x)$ is a polynomial of degree ____.

- -

ANSWER:

one or two.

- -

POLYNOMIALS OVER OTHER FIELDS

Mathematicians often find it convenient to consider polynomials over fields other than the fields of rational numbers, real numbers, and complex numbers. We have learned previously that the system $I/2$ of integers modulo 2 is a field. Recall that this field contains only two elements, 0 and 1. Addition and multiplication in this field are defined as follows:

(a)		(b)	
	$0 + 0 = 0$		$0 \cdot 0 = 0$
	$0 + 1 = 1$		$0 \cdot 1 = 0$
	$1 + 0 = 1$		$1 \cdot 0 = 0$
	$1 + 1 = 0$		$1 \cdot 1 = 1$

The domain of any polynomial function over $I/2$ is ____.

- -

ANSWER:

I/2, or {0, 1}.

- -

The range of any polynomial function over I/2 is ____.

- -

ANSWER:

A subset of I/2. Therefore the range must be either {0} or {1} or {0, 1}. Note that the answers "I/2" and "{0, 1}" are not correct.

- -

How many functions (polynomial functions or not) are there with domain {0, 1} and range {0}? List them.

- -

ANSWER:

Only one; the function $F = \{(0, 0), (1, 0)\}$, or F: $0 \longrightarrow 0$
$1 \longrightarrow C$.

- -

Is this a polynomial function?

- -

ANSWER:

Yes, it is the zero polynomial function. Any constant function from I/2 to I/2 is a polynomial function.

- -

How many functions (polynomial functions or not) are there with domain {0, 1} and range {1}? List them.

- -

ANSWER:

Only one; the function G = {(0, 1), (1, 1)}, or G: $0 \longrightarrow 1$
$1 \longrightarrow 1$

- -

Is this a polynomial function?

- -

ANSWER:

Yes, a constant polynomial function.

- -

List the ordered pairs in the polynomial functions, P and Q, determined by the polynomials P(x) = x and Q(x) = x + 1 (over I/2).

- -

ANSWER:

P = {(0, 0), (1, 1)}
Q = {(0, 1), (1, 0)}

- -

Are there any functions other than P, Q with domain {0, 1} and range {0, 1}? If so, list them.

- -

ANSWER:

There are none.

- -

We conclude that over the field I/2 there are exactly ____ polynomial functions.

- -

ANSWER:

four; the functions F, G, P, and Q described above.

- -

List all the polynomials over I/2 of degree 2.

- -

ANSWER:

(i) x^2

(ii) $x^2 + 1$

(iii) $x^2 + x$

(iv) $x^2 + x + 1$

- -

Which polynomial over I/2 of degree 2 determines the zero polynomial function?

- -

ANSWER:

$x^2 + x$.

- -

Find all the roots in I/2 of the following polynomials over I/2.

(a) $x^3 + x^2$

(b) $x^4 + x^2 + x + 1$

(c) $x^4 + x^2 + 1$

- -

ANSWER:

(a) 0 and 1; $0^3 + 0^2 = 0 + 0 = 0$, $1^3 + 1^2 = 1 + 1 = 0$

(b) 1; $0^4 + 0^2 + 0 + 1 = 0 + 0 + 0 + 1 = 1 \neq 0$, $1^4 + 1^2 + 1 + 1 = 0$

(c) no roots; $0^4 + 0^2 + 1 = 0 + 0 + 1 = 1 \neq 0$,
$1^4 + 1^2 + 1 = 1 + 1 + 1 = 1 \neq 0$.

- -

Add the polynomials $x^3 + x^2 + 1$ and $x^2 + x + 1$, over I/2. (Recall that the exponents on x are non-negative integers, not elements of the field I/2. Hence the exponents 2 and 3 are permitted.)

- -

ANSWER:
$(x^3 + x^2 + 1) + (x^2 + x + 1) = x^3 + (1 + 1)x^2 + x + (1 + 1) =$
$x^3 + x$. Remember that $1 + 1 = 0$ in I/2.

- -

By multiplication show that $(x + 1)(x + 1)(x + 1)$ is a factorization of $x^3 + x^2 + x + 1$.

- -

ANSWER:
$(x + 1)(x + 1) = x^2 + (1 + 1)x + 1 = x^2 + 1$.
$(x + 1)(x + 1)(x + 1) = (x^2 + 1)(x + 1) = x^3 + x^2 + x + 1$.

- -

We know that if c is a root of a polynomial $P(x)$, then $x - c$ is a factor. In this case $P(x)$ can be factored by dividing $P(x)$ by $x - c$, using long division. However, in the division process we must be careful to remember that we are working with the field I/2. Let us illustrate.

Let $P(x) = x^4 + x^2 + x + 1$. Is 1 a root of $P(x)$?

- -

ANSWER:
Yes.

- -

We divide $P(x)$ by $x - 1$.

$$
\begin{array}{r|rrrrr}
 & & x^3 & +x^2 & & +1 \\ \hline
x - 1 & x^4 & & +x^2 & +x & +1 \\
 & x^4 & -x^3 & & & \\
 & (-) & (+) & & & \\ \cline{2-6}
 & 0 & +x^3 & +x^2 & & \\
 & & x^3 & -x^2 & & \\
 & & (-) & (+) & & \\ \cline{2-6}
 & & 0 & +0 & +x & +1 \\
 & & & & x & -1 \\
 & & & & (-) & (+) \\ \cline{4-6}
 & & & & 0 & +0
\end{array}
$$

Then we can factor $P(x)$ as follows:

$$x^4 + x^2 + x + 1 = (x - 1)(x^3 + x^2 + 1).$$

Is $x - 1$ the same as $x + 1$?

- -

ANSWER:

Yes. In I/2, $-1 = +1$. (-1 is the additive inverse of 1.)

- -

Therefore we could also write

$$x^4 + x^2 + x + 1 = (x + 1)(x^3 + x^2 + 1).$$

Factor the polynomial $x^4 + x^3 + x^2 + 1$ as a product of a polynomial of degree 1 and a polynomial of degree 3 (over I/2).

- -

ANSWER:

1 is a root of $x^4 + x^3 + x^2 + 1$. So $x - 1$ is a factor. Dividing, we obtain

$$
\begin{array}{rrl}
 & & \underline{x^3 + x \ + 1} \\
x - 1 & & \big)\, x^4 + x^3 + x^2 + 1 \\
 & & x^4 - x^3 \\
 & (-) & \underline{\quad (+) \qquad\qquad\qquad} \\
 & & 0 + 0 + x^2 \\
 & & \qquad\qquad x^2 - x \\
 & & \qquad\quad \underline{(-) \ \ (+)} \\
 & & \qquad\qquad 0 + x + 1 \\
 & & \qquad\qquad\quad x - 1 \\
 & & \qquad\qquad \underline{(-) \ \ (+)} \\
 & & \qquad\qquad\quad 0 + 0
\end{array}
$$

Hence $x^4 + x^3 + x^2 + 1 = (x - 1)(x^3 + x + 1)$

or $x^4 + x^3 + x^2 + 1 = (x + 1)(x^3 + x + 1)$

- -

The system I/3 of integers modulo 3 is a field. I/3 = {0, 1, 2}. Following are the addition and multiplication tables for I/3.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

There are three constant functions from I/3 to I/3. List them.

- -

ANSWER:

F = {(0, 0), (1, 0), (2, 0)}, G = {(0, 1), (1, 1), (2, 1)}, and H = {(0, 2), (1, 2), (2, 2)}; or

F: $0 \longrightarrow 0$ G: $0 \longrightarrow 1$ H: $0 \longrightarrow 2$
$1 \longrightarrow 0$ $1 \longrightarrow 1$ $1 \longrightarrow 2$
$2 \longrightarrow 0$ $2 \longrightarrow 1$ $2 \longrightarrow 2$

- -

Are these functions polynomial functions over $I/3$?

ANSWER:

Yes, they are constant polynomial functions.

List the ordered pairs in the function determined by the polynomial $2x^2 + x + 1$.

ANSWER:

$(0, 1)$, $(1, 1)$, $(2, 2)$.

Write in factored form a polynomial over $I/3$ of degree 3 which has 0, 1, and 2 as roots.

ANSWER:

$(x - 0)(x - 1)(x - 2) = x(x + 2)(x + 1)$

$2x(x + 1)(x + 2)$ is also correct.

Write the polynomial $x(x + 2)(x + 1)$ in the form $ax^3 + bx^2 + cx + d$.

ANSWER:

$x(x + 2)(x + 1) = 1 \cdot x^3 + 0 \cdot x^2 + 2 \cdot x + 0 = x^3 + 2x$.

What is the polynomial function over $I/3$ determined by the polynomial $x^3 + 2x$?

ANSWER:

The zero polynomial function.

- -

Find all the roots in I/3 of the polynomial $x^4 + 2x^3 + 2x$.

- -

ANSWER:

0 and 2.

$0^4 + 2(0)^3 + 2 \cdot 0 = 0 + 0 + 0 = 0$

$1^4 + 2 \cdot 1^3 + 2 \cdot 1 = 1 + 2 + 2 = 2 \neq 0$

$2^4 + 2 \cdot 2^3 + 2 \cdot 2 = 1 + 1 + 1 = 0$

- -

Suppose the polynomial $x^3 + x^2 + 2x + 1$ is factorable over I/3. Then it can be factored as a product of two factors, one of which has degree ____ and the other has degree ____.

- -

ANSWER:

two

one.

- -

Does the polynomial $x^3 + x^2 + 2x + 1$ have a root in I/3?

- -

ANSWER:

No.

- -

Can we conclude that $x^3 + x^2 + 2x + 1$ is irreducible over I/3? Explain.

- -

ANSWER:

Yes. If $x^3 + x^2 + 2x + 1$ were factorable over I/3 it would have a factor of degree 1 and would therefore have a root in I/3.

- -

List all the polynomials of degree 2 over I/3 which have $2x$ as one term.

- -

ANSWER:

$x^2 + 2x$	$2x^2 + 2x$
$x^2 + 2x + 1$	$2x^2 + 2x + 1$
$x^2 + 2x + 2$	$2x^2 + 2x + 2$

- -

Using long division, divide the polynomial $x^3 + x^2 + 1$ by $2x + 1$ (over I/3).

- -

ANSWER:

$$\begin{array}{r l}
 & \;\; 2x^2 + x + 1 \\
2x + 1 & \big) \overline{\, x^3 + x^2 \quad +1 \qquad} \\
 & \;\; \underline{x^3 + 2x^2} \\
 & \qquad -x^2 \\
 & \qquad \underline{\;\; 2x^2 + x} \\
 & \qquad\qquad -x + 1 \\
 & \qquad\qquad \underline{2x + 1} \\
 & \qquad\qquad\qquad 0
\end{array}$$

Note that 2 is the coefficient of x^2 in the quotient because 2 is the multiplicative inverse of 2; i.e., $2 \cdot 2 = 1$ (in I/3).

- -

Following are the addition and multiplication tables for I/5.

Addition

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

List the ordered pairs in the polynomial function P determined by the polynomial $x^5 + 3x^4 + 2$ over $I/5$.

ANSWER:

$\{(0, 2), (1, 1), (2, 2), (3, 3), (4, 4)\}$.

List the ordered pairs in the polynomial function Q determined by the polynomial $3x^4 + x + 2$ over $I/5$.

ANSWER:

$\{(0, 2), (1, 1), (2, 2), (3, 3)\ (4, 4)\}$.

Therefore P and Q are the same function. We have shown that, over the field $I/5$, different polynomials do not always determine different polynomial functions.

Find all the roots in $I/5$ of the polynomial $x^4 + x^3 + 4x + 4$ over $I/5$.

ANSWER:

1 and 4.

Divide the polynomial $x^4 + 2x^3 + 4x^2 + 2$ by $2x + 1$. In dividing remember that you are working with I/5.

The first step in the process is given as follows:

$$\begin{array}{rl}
 & \quad 3x^3 \\
2x + 1 & \overline{)\, x^4 + 2x^3 + 4x^2 + 2} \\
 & \underline{x^4 + 3x^3} \\
 & \qquad -x^3 + 4x^2
\end{array}$$

Note that the coefficient of x^3 in the quotient is 3 because ____.

- -

ANSWER:

3 is the multiplicative inverse of 2 in I/5, or $2 \cdot 3 = 1$ in I/5.

- -

Complete the division.

- -

ANSWER:

$$\begin{array}{rl}
 & \quad 3x^3 + 2x^2 + x + 2 \\
2x + 1 & \overline{)\, x^4 + 2x^3 + 4x^2 + 2} \\
 & \quad x^4 + 3x^3 \\
 & \underline{(-) \quad (-) \qquad\qquad\quad} \\
 & \qquad -x^3 + 4x^2 \\
 & \qquad 4x^3 + 2x^2 \\
 & \qquad \underline{(-) \quad (-) \qquad} \\
 & \qquad\quad 0 + 2x^2 \\
 & \qquad\qquad 2x^2 + x \\
 & \qquad\qquad \underline{(-) \quad (-)} \\
 & \qquad\qquad\qquad -x + 2 \\
 & \qquad\qquad\qquad 4x + 2 \\
 & \qquad\qquad\qquad \underline{(-) \quad (-)} \\
 & \qquad\qquad\qquad\qquad 0
\end{array}$$

Note that $-x^3 = (-1) \cdot x^3 = 4x^3$ because 4 is the additive inverse of 1. Similarly $-x = 4x$.

- -

Is the quotient $3x^3 + 2x^2 + x + 2$ of the previous division irreducible over I/5? If not, find a factor of degree 1.

- -

ANSWER:

No; $x - 4$ or $x + 1$. Over I/5, $x - 4$ and $x + 1$ are the same polynomial.

- -

We should remark here that, in general, the problem of finding the roots or the irreducible factors of a polynomial over a field is very difficult. If the field is finite and does not have too many elements we can find the roots of a polynomial over the field by substituting each element of the field in place of x in the polynomial.

If K is any field then each polynomial $P(x)$ over K determines a unique polynomial function P over K. Thus the polynomial $P(x) = x^2 + 2$ over I/3 determines what polynomial function?

- -

ANSWER:

$P = \{(0, 2), (1, 0), (2, 0)\}$, or

$P: 0 \longrightarrow 2$
$\quad 1 \longrightarrow 0$
$\quad 2 \longrightarrow 0$

- -

We can define a function ϕ as follows:

$\phi: P(x) \longrightarrow P$, for each polynomial $P(x)$ over K.

Here P is the polynomial function determined by the polynomial $P(x)$. $P(x)$ is an element of the set ____ while P is an element of the set ____.

ANSWER:

of polynomials over K

of polynomial functions over K.

The domain of ϕ is ____.

ANSWER:

the set of polynomials over K.

Since every polynomial function over K is determined by some polynomial over K, the range of ϕ is ____.

ANSWER:

the set of all polynomial functions over K.

Let K be the field I/2 and let $P(x) = x^2 + 1$, $Q(x) = x + 1$. Find the polynomial functions P and Q determined by the polynomials $P(x)$ and $Q(x)$.

ANSWER:

P:	$0 \longrightarrow 1$	Q:	$0 \longrightarrow 1$
	$1 \longrightarrow 0$		$1 \longrightarrow 0$

Under the function ϕ, $P(x) \longrightarrow$ ____ and $Q(x) \longrightarrow$ ____.

ANSWER:

P, Q.

Is the function ϕ reversible?

ANSWER:

No. $P(x) \neq Q(x)$ but $P = Q$. Thus $(P(x), P)$ and $(Q(x), Q)$ are distinct ordered pairs in the function ϕ with the same second member.

We see that over the field I/2, distinct polynomials do not necessarily determine distinct polynomial functions. The same is true for the fields I/3 and I/5 and indeed for every field with only a finite number of elements.

In working with polynomials over the fields of rational numbers, real numbers, or complex numbers, there is no great reason for making a distinction between polynomials and polynomial functions. This is due to the following theorem.

THEOREM 13.9: Over the fields of rational numbers, real numbers, and complex numbers, if $P(x)$ and $Q(x)$ are different polynomials then they determine different polynomial functions.

Let us consider real polynomials. Let ϕ be the set of all ordered pairs of the form $(P(x), P)$, such that $P(x)$ is a real polynomial and P is the unique real polynomial function determined by $P(x)$. ϕ is a function. What can you conclude from Theorem 13.9 about the function ϕ?

ANSWER:

ϕ is a reversible function.

Therefore the function ϕ defined by $P(x) \xrightarrow{\phi} P$ is a one-to-one mapping from the set ____ onto the set ____.

ANSWER:

of real polynomials
of real polynomial functions.

If $P(x)$ and $Q(x)$ are real polynomials and $P(x) \xrightarrow{\phi} P$, and $Q(x) \xrightarrow{\phi} Q$, then $P(x) + Q(x) \xrightarrow{\phi}$ ____ and $P(x) \cdot Q(x) \xrightarrow{\phi}$ ____.

ANSWER:

$P + Q$
$P \cdot Q$

Therefore ϕ is a(n) ____ from the system of real polynomials onto the system of real polynomial functions.

ANSWER:

isomorphism

Because of the above isomorphism many books do not distinguish between polynomials and polynomial functions. For example, the Ball State curriculum materials define polynomial functions as we have, and call the polynomial functions themselves polynomials. In a course where one considers only polynomials over the number fields, it is perhaps best not to make a distinction between polynomials and polynomial functions.

You should be careful to note, however, that for polynomials over many fields (such as $I/2$ and $I/5$, for example) there is no isomorphism as described above.

Let us try to prove Theorem 13.9 for the field of rational numbers. If $P(x)$ and $Q(x)$ are rational polynomials which determine the same polynomial function, then ____ for every rational number c.

- -

ANSWER:

$P(c) = Q(c)$

- -

This implies that every rational number c is a root of the polynomial ____.

- -

ANSWER:

$P(x) - Q(x)$.

- -

If $P(x) \neq Q(x)$, why does this contradict Theorem 13.5?

- -

ANSWER:

If $P(x) \neq Q(x)$, then $P(x) - Q(x)$ is a non-zero polynomial. If it has degree k, Theorem 13.5 says that it cannot have more than k distinct roots. So it cannot have every rational number as a root.

- -

You may observe that the above proof works equally well if, instead of the rational field, we use any field with an infinite number of elements.

Let us assume now that K is a field and that L is a field containing K as a subfield. For example, we could take L to be the field of complex numbers and K to be the field of real numbers, or rational numbers. If c is an element of L then it may or may not be true that there is a non-zero polynomial over K which has c as a root. We make the following definitions.

DEFINITION 13.13: Let K be a subfield of a field L, and let c be an element of L. Then c is said to be algebraic over K if there is a non-zero polynomial over K which has c as a root. If c is not algebraic over K then it is said to be transcendental over K.

Let us illustrate this definition with examples.

Find a non-zero polynomial over the field of rational numbers which has $\sqrt{2}$ as a root.

- -

ANSWER:

e.g., $x^2 - 2$

- -

Thus we say that $\sqrt{2}$ is ____ (algebraic or transcendental) over the field of rational numbers.

- -

ANSWER:

algebraic

- -

It can be proved that there is no non-zero rational polynomial which has the number π as root. Therefore π is ____ over the field of rational numbers.

- -

ANSWER:

transcendental

- -

Is the complex number i algebraic over the field of real numbers?

- -

ANSWER:

Yes; i is a root of the non-zero real polynomial $x^2 + 1$.

- -

Is the complex number i algebraic over the field of rational numbers?

- -

ANSWER:

Yes; $x^2 + 1$ is also a rational polynomial. So $x^2 + 1$ is a non-zero rational polynomial having i as a root.

- -

Consider the complex numbers:

(a) $-2i$

(b) $-\sqrt{2}\, i$

(c) πi

(d) $1 + i$

(1) Which of these numbers are algebraic over the field of real numbers? ____.

(2) Which of these numbers are algebraic over the field of rational numbers? ____.

- -

ANSWER:

(1) (a), (b), (c), (d).

(2) (a), (b), (d).

- -

Let c be a complex number. Find a real polynomial which has c as a root.

ANSWER:

e.g., $(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c \cdot \bar{c}$. Recall that $c + \bar{c}$ and $c \cdot \bar{c}$ are real numbers.

We conclude that every complex number c is ____ over the field of real numbers.

ANSWER:

algebraic

Suppose K is a subfield of a field L and c is an element of L. Let $P(x)$ and $Q(x)$ be distinct polynomials over K and assume that $P(c) = Q(c)$. Find a non-zero polynomial over K which has c as a root.

ANSWER:

$P(x) - Q(x)$ is a non-zero polynomial because $P(x)$ and $Q(x)$ are distinct. Moreover, c is a root of $P(x) - Q(x)$ because $P(c) - Q(c) = 0$.

Refer to the preceding item. Is c transcendental over K?

ANSWER:

No.

We can conclude that if c is transcendental over K, then $P(c) \neq Q(c)$ whenever $P(x)$ and $Q(x)$ are distinct polynomials. Thus, if

$$a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c + a_0 = b_m c^m + b_{m-1} c^{m-1} + \ldots + b_1 c + b_0$$

and $a_n \neq 0$, $b_m \neq 0$, then $n = m$ and $a_0 = b_0$, $a_1 = b_1$, $\ldots a_n = b_n$.

This shows that if c is transcendental over a field K, then c has the basic property that was required of the "variable" x in Definition 13.2. The definition of polynomial given in Definition 13.1 can be made logically precise by specifying that x is an element which is transcendental over K; i.e., x is an element of a field containing K as a subfield with the property that if $(a_0, a_1, \ldots, a_n)$ is a sequence of elements from K such that

$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$, then $a_0 = 0$, $a_1 = 0$, $\ldots$, $a_n = 0$. It can be proved, though we shall not do so here, that if K is any field there does exist a field L containing K as a subfield and which contains an element transcendental over K.

REVIEW ITEMS

1. If a polynomial has a multiplicative inverse which is a polynomial then it is called a ____.

- -

ANSWER:

unit.

- -

2. If a polynomial is a unit it has degree ____.

- -

ANSWER:

zero.

- -

3. Give the leading coefficient and degree of each of the following polynomials.

(a) $3x^5 - 2x^3 + 1$

(b) $x - 4$

(c) 0

(d) $\sqrt{3}$

- -

ANSWER:

	Leading Coefficient	Degree
(a)	3	5
(b)	1	1
(c)	has none	has none
(d)	$\sqrt{3}$	0

- -

4. A polynomial which is irreducible over the field of complex numbers must have degree ____ while a polynomial which is irreducible over the field of real numbers must have degree ____.

- -

ANSWER:

one

one or two.

- -

5. Does every constant polynomial have degree zero?

- -

ANSWER:

No. The zero polynomial is a constant polynomial but it has no degree.

- -

6. Which of the following polynomials are (1) units, (2) irreducible over the real numbers, (3) factorable over the real numbers?

(a) $4x^2 + 4$

(b) -37

(c) $x^2 - 2$

(d) $2x + 1$

- -

ANSWER:

(1) (b).

(2) (a) and (d).

(3) (c).

- -

7. (a) List the defining properties of an integral domain.

(b) Which of these properties, if any, does the system of all real polynomials with zero constant term possess?

- -

ANSWER:

(a) An integral domain is a set with two closed binary operations (addition and multiplication) with properties: A_a, A_c, A_{id}, A_{in}, M_a, M_c, M_{id}, D, and the cancellation properties for multiplication.

(b) This system possesses all these properties except M_{id}.

- -

8. Suppose $3 - 2i$ is a root of a real polynomial. Find a real factor of degree 2 of the polynomial.

- -

ANSWER:

$x^2 - 6x + 13$. Since $3 - 2i$ is a root, $\overline{3 - 2i} = 3 + 2i$ is also a root. Hence $x - [3 - 2i]$ and $x - [3 + 2i]$ are complex factors. Then $(x - [3 - 2i])(x - [3 + 2i]) = x^2 - 6x + 13$ is a real factor.

- -

9. If $P(x)$ is a polynomial of degree m and $Q(x)$ is a polynomial of degree n the degree of $P(x) \cdot Q(x)$ is ____.

- -

ANSWER:

$m + n$.

- -

10. If $P(x)$ has degree 7 and $Q(x)$ has degree 5, what is the degree of $P(x) + Q(x)$?

- -

ANSWER:

7.

- -

11. If $P(x)$ has degree 7 and $Q(x)$ has degree 7, what can you say about the degree of $P(x) + Q(x)$?

- -

ANSWER:

If $P(x) + Q(x) \neq 0$, then $P(x) + Q(x)$ has degree less than or equal to 7. If $P(x) + Q(x) = 0$, then $P(x) + Q(x)$ has no degree.

- -

12. If $P(x)$ has degree m, $Q(x)$ has degree n, and $m > n$, then $P(x) + Q(x)$ has degree ____.

- -

ANSWER:

m.

- -

13. If $P(x)$ and $Q(x)$ each have degree n then what can you say about the degree of $P(x) + Q(x)$?

- -

ANSWER:

If $P(x) + Q(x) \neq 0$, then the degree of $P(x) + Q(x)$ is less than or equal to n. If $P(x) + Q(x) = 0$, then $P(x) + Q(x)$ has no degree.

- -

14. Let $P(x) = 3x^3 - 2x^2 + x + 1$ and $N(x) = x + 2$. Then $P(x) = (3x^2 - 8x + 1)N(x) + (16x - 1)$. Is it true that if we divide $P(x)$ by $N(x)$ using the Division Theorem for polynomials that the quotient is $3x^2 - 8x + 1$ and the remainder is $16x - 1$? Explain.

- -

ANSWER:

No. The remainder obtained by applying the Division Theorem must either be zero or have degree less than the degree of $N(x)$. In the given example $16x - 1$ does not have degree less than the degree of $N(x)$.

- -

15. Suppose $P(x)$ and $N(x)$ are non-zero polynomials and $P(x)$ has degree greater than or equal to the degree of $N(x)$. In dividing $P(x)$ by $N(x)$ using long division the first step is to look for a monomial cx^k such that ____.

- -

ANSWER:

$P(x) - cx^k N(x)$ has degree less than the degree of $P(x)$.

---

16. The first step in the division of $P(x) = x^4 - 2x^3 + 3x^2 + x - 1$ by $N(x) = x^2 + 2$ is

$$\begin{array}{r|l} & x^2 \\ \cline{2-2} x^2 + 2 & x^4 - 2x^3 + 3x^2 + x - 1 \\ & \underline{x^4 \qquad\quad + 2x^2 \qquad\qquad} \\ & \quad\; - 2x^3 + x^2 + x - 1 \end{array}$$

This gives us the following representation for $P(x)$:

$x^4 - 2x^3 + 3x^2 + x - 1 =$ ____.

ANSWER:

$x^2 \cdot (x^2 + 2) + (-2x^3 + x^2 + x - 1)$.

---

17. Can an irreducible polynomial have degree 0?

ANSWER:

No; by definition, an irreducible polynomial is non-constant.

---

18. In the Standard Factorization Theorems for integers and polynomials what polynomials are the analogues of the positive prime integers?

ANSWER:

The irreducible polynomials with leading coefficient one (irreducible monic polynomials).

---

19. Find the standard factorization for each of the following polynomials over the rational numbers.

(a) $-x^3 + x$

(b) $(1/2)(x^2) + x + 1/2$

(c) 3

(d) $2x^2 - 4$

ANSWER:

(a) $(-1)x(x - 1)(x + 1)$

(b) $(1/2)(x + 1)(x + 1)$

(c) 3 is a unit; therefore it has no standard factorization

(d) $2(x^2 - 2)$

---

20. Suppose $P(x) = Q_1(x) \cdot Q_2(x) \ldots Q_k(x)$, where each of $Q_1(x)$, $Q_2(x), \ldots, Q_k(x)$ is irreducible. Denote the leading coefficient of $Q_1(x)$ by c_1, the leading coefficient of $Q_2(x)$ by c_2, etc. What is the standard factorization of $P(x)$?

ANSWER:

Let $c = c_1c_2 \ldots c_k$. Then $P(x) = c \cdot (\frac{1}{c_1}Q_1(x)) \cdot (\frac{1}{c_2}Q_2(x)) \ldots (\frac{1}{c_k}Q_k(x))$.

---

21. Without actually dividing find the remainder obtained in each of the following divisions.

(a) $x^6 + 2x^3 - 1$ by $x - \sqrt[3]{5}$.

(b) $x^{37} - 2x^{14} + 4$ by $x + 1$.

- -

ANSWER:

(a) 34

(b) 1

- -

22. Using the factor theorem find a factor of degree one of each of the following polynomials.

(a) $x^{17} + 2^{17}$.

(b) $x^{20} - x^{18} + x + 1$.

- -

ANSWER:

(a) $x + 2$

(b) $x + 1$

- -

23. Is $x + 1$ a factor of $x^n + x^{n-1} + x^{n-2} + \dots + x + 1$ if n is an even positive integer? ____. If n is an odd positive integer? ____.

- -

ANSWER:

No.

Yes.

- -

24. If $P(x) = (x - c)Q(x)$, how are the roots of $P(x)$ and $Q(x)$ related?

- -

ANSWER:

Each root of $Q(x)$ is a root of $P(x)$. Each root of $P(x)$, except possibly for c, is a root of $Q(x)$.

- -

25. If $P(x)$ is a polynomial which has every positive integer as root, what can you say about $P(x)$? Explain.

- -

ANSWER:

$P(x) = 0$. By Theorem 13.5, if $P(x) \neq 0$ and has degree n it cannot have more than n distinct roots.

- -

26. Give the standard factorization of the polynomial $3x^4 - 27$, (a) over the rational numbers, (b) over the real numbers, and (c) over the complex numbers.

- -

ANSWER:

(a) $3(x^2 - 3)(x^2 + 3)$.

(b) $3(x - \sqrt{3})(x + \sqrt{3})(x^2 + 3)$

(c) $3(x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{3}i)(x + \sqrt{3}i)$.

- -

27. What theorem can be used to deduce that every complex number has an n^{th} root for every positive integer n? Explain. (An n^{th} root of a complex number a is a complex number b such that $b^n = a$.)

- -

ANSWER:

Theorem 13.7, the Fundamental Theorem of Algebra. This theorem says that every complex polynomial has a root in the field of complex numbers. If a is a complex number and n is a positive integer then the polynomial $x^n - a$ has a root, which is an n^{th} root of a.

- -

28. Find all the roots in $I/5$ of the polynomial $x^4 + x + 2$, over $I/5$.

- -

ANSWER:

2 is the only root.

---

29. Factor the polynomial $x^4 + x + 2$ over I/5 in the form $(x + 3)Q(x)$.

ANSWER:

Dividing $x^4 + x + 2$ by $x + 3$, using long division, we get

$$x^4 + x + 2 = (x + 3)(x^3 + 2x^2 + 4x + 4).$$

---

30. The polynomial $x^3 + 2x^2 + 4x + 4$ over I/5 has no root in I/5. Can we conclude that it is irreducible over I/5? Explain.

ANSWER:

Yes; if $x^3 + 2x^2 + 4x + 4$ were factorable, it could be factored as a product of a polynomial of degree 2 and a polynomial of degree 1. If it had a factor of degree 1, it would have a root.

---

31. Write down all polynomials over I/3 which have degree 3 and which have the terms $2x^2 + x$.

ANSWER:

$x^3 + 2x^2 + x$

$x^3 + 2x^2 + x + 1$

$x^3 + 2x^2 + x + 2$

$2x^3 + 2x^2 + x$

$2x^3 + 2x^2 + x + 1$

$2x^3 + 2x^2 + x + 2$

---

32. Find the polynomial function determined by each of the polynomials $2x^2 + 2x + 2$ and $x^3 + 2x^2 + x + 2$ over I/3.

ANSWER:

Each polynomial determines the polynomial function P defined by:

$$\begin{aligned} P:\ & 0 \longrightarrow 2 \\ & 1 \longrightarrow 0 \\ & 2 \longrightarrow 2 \end{aligned}$$

---

33. The polynomial $x^4 + x^2 + 4$ over I/5 has no root in I/5. Can we conclude that it is irreducible over I/5? Explain.

ANSWER:

No. Since it has no roots in I/5, it can not have any factors of degree 1. However it does factor into factors of degree 2:

$$x^4 + x^2 + 4 = (3x^2 + 4)(2x^2 + 1)$$

---

34. Factor the polynomial $x^3 + 3x^2 + 4x + 2$ into irreducible factors over I/5.

ANSWER:

$(x + 1)(x + 4)(x + 3)$. Note that $x + 1 = x - 4$, $x + 4 = x - 1$, and $x + 3 = x - 2$, over I/5.

---

35. Let ϕ be the function defined by $\phi: P(x) \longrightarrow P$, for each rational polynomial $P(x)$, where P is the rational polynomial function determined by $P(x)$.

ϕ is a function from the set ____ onto the set ____. Is ϕ an isomorphism?

ANSWER:

of rational polynomials

of rational polynomial functions

Yes.

---

36. Which of the following complex numbers are algebraic over the field of rational numbers?

(a) 2

(b) $\sqrt[2]{3}$

(c) π

(d) $2i$

(e) πi

(f) 0

ANSWER:

(a), (b), (d), (f).

---

37. Let $c = a + bi$ (a and b real numbers) be a complex number. Find a real polynomial which has c as a root.

ANSWER:

$(x - c)(x - \overline{c}) = x^2 - 2ax + a^2 + b^2$.

---

38. Is there a complex number which is transcendental over the field of real numbers?

ANSWER:

No; every complex number is a root of some quadratic real polynomial.

XIV. EQUIVALENCE RELATIONS AND GROUPS

PROPERTIES OF RELATIONS

In Unit I we defined the *Cartesian product* of non-empty sets X and Y, written X × Y, to be the set of all ordered pairs (x, y) such that x is an element of X and y is an element of Y.

A non-empty subset of X × Y we have called a ____ between X and Y.

- -

ANSWER:

relation

- -

If S is a non-empty set, a non-empty subset of S × S is a relation between S and S. This is the situation above where X and Y are the same set S. In this case we usually say "relation in S" instead of "relation between S and S." *Thus a relation in a set* S is a non-empty set R where each element of R is an ordered pair (x, y) with x and y elements of S. When R is a relation and (x, y) is an ordered pair in R we will often write "x R y" and say "x is R-related to y".

DEFINITION 14.1: If R is a relation in a set S, then R is *reflexive in* S if and only if (a, a) is an element of R for every element a in S.

Note that the reflexive property is not a property of R alone, but of R and the set S.

To show that a binary relation R in a set S is reflexive in S, you must show that ____ for each a in S.

ANSWER:

(a, a) is in R.

To show that a binary relation R in a set S is not reflexive in S, you need to find only one a in S for which ___.

ANSWER:

(a, a) is not in R.

Let S = {1, 2, 3, 4}
and R = {(1, 1), (2, 2), (2, 4), (3, 3), (4, 1), (4, 4)}.

Is it true that (x, x) is in R for every x in S? ____

Therefore R ____ (is or is not) reflexive in S.

ANSWER:

Yes
is

Let S = {1, 2, 3, 4}
and R = {(1, 1), (2, 2), (2, 3), (4, 4)}

Is it true that (x, x) is in R for every x in S? ____

Therefore R ____ (is or is not) reflexive in S.

ANSWER:

No, 3 is in S, but (3, 3) is not in R.

is not

- -

Let S = {1, 2, 3}

and R = {(1, 1), (2, 1), (3, 1), (3, 3)}

Is R reflexive in S? If not, why?

- -

ANSWER:

No; 2 is in S, but (2, 2) is not in R.

- -

Let S be the set of all real numbers, and let R be the set of all ordered pairs of positive numbers (a, b), such that a = b. Is R reflexive in S? If not, why?

- -

ANSWER:

No; for example, -3 is in S, but (-3, -3) is not in R.

- -

If, in the example above, S were the set of all positive numbers, would R be reflexive in S?

- -

ANSWER:

Yes.

- -

Let S = {a, b, c, d}. A binary relation R in S would have to contain at least ____ elements in order to be reflexive.

- -

ANSWER:

four (although it could contain more).

Let S be the set of all lines in a plane, and $\mathcal{R}$ be the set of all ordered pairs (ℓ, m) such that ℓ and m are lines and ℓ is perpendicular to m. Is $\mathcal{R}$ a reflexive relation in S?

ANSWER:

No (a line is not perpendicular to itself).

DEFINITION 14.2: A relation $\mathcal{R}$ in a set S is symmetric if and only if whenever an ordered pair (a, b) is in $\mathcal{R}$, the ordered pair (b, a) is also in $\mathcal{R}$ (or, if $a \mathcal{R} b$, then $b \mathcal{R} a$).

Let $S = \{a, b, c\}$

and $\mathcal{R} = \{(a, b), (b, a), (b, c), (c, b)\}$

Is $\mathcal{R}$ symmetric? If not, why?

ANSWER:

Yes.

Let $S = \{1, 2, a, b\}$

and $\mathcal{R} = \{(1, a), (a, 1), (1, b)\}$

Is $\mathcal{R}$ symmetric? If not, why?

ANSWER:

No; $(1, b)$, is in $\mathcal{R}$, but $(b, 1)$ is not in $\mathcal{R}$.

Let S = {1, 2, 3, 4}
and R = {(3, 3)}

Is R symmetric? If not, why?

Is R reflexive in S? If not, why?

- -

ANSWER:

Yes.

No; 1, 2, and 4 are in S but (1, 1), (2, 2), and (4, 4) are not in R.

- -

Given a relation R in a set S:

To decide if R is reflexive, you must check that for every x in ____, (x, x) is in ____.

To decide if R is symmetric, you must check that for every (x, y) in ____, ____ is in R.

- -

ANSWER:

S; R

R; (y, x)

- -

Let S be the set of all plane angles in geometry, and let R be the set of all ordered pairs of angles (A, B) such that angle A is supplementary to angle B. Is R a symmetric relation in S?

- -

ANSWER:

Yes.

- -

DEFINITION 14.3: A relation R in a set S is said to be *transitive* if and only if it satisfies the condition: whenever (x, y) is in R and (y, z) is in R, then (x, z) is also in R (or, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$).

Let $S = \{1, 2, 3, 4\}$
and $R = \{(1, 2), (2, 3), (3, 4)\}$.

Why is R not transitive?

ANSWER:
The ordered pairs $(1, 2)$ and $(2, 3)$ are in R but $(1, 3)$ is not in R. (Take $x = 1$, $y = 2$, $z = 3$ in Definition 14.3).

Or, the ordered pairs $(2, 3)$ and $(3, 4)$ are in R but $(2, 4)$ is not in R. (Take $x = 2$, $y = 3$, $z = 4$ in Definition 14.3).

Let $S = \{a, b, c\}$
and $R = \{(a, b), (b, a), (a, a)\}$

Is R transitive? If not, why?

ANSWER:
No. You may think that R is transitive because of the order in which we have listed the elements in R. Since (b, a) and (a, b) are in R, and (b, b) is not in R, then R is not transitive.

Let $S = \{4, 7, 9, 10\}$
and $R = \{(4, 7), (7, 9), (4, 9), (7, 4), (4, 4)\}$

Is R transitive? If not, why?

ANSWER:

No; for example, (7, 4) and (4, 7) are in R, but (7, 7) is not.

Let S be the set of all lines in a plane and let R be the relation in S consisting of all ordered pairs (ℓ, m) where ℓ is either the same line as m or ℓ is parallel to m. Is R a transitive relation?

ANSWER:

Yes. Recall that if ℓ, m, and n are lines and if ℓ is parallel to m and m is parallel to n then either ℓ is the same as n or ℓ is parallel to n.

Let $S = \{a, b, c, d\}$

and $R = \{(a, a), (a, b), (b, d), (a, d)\}$

Is R transitive? If not, why?

ANSWER:

Yes.

Let S be the set of integers and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and $x \cdot y \geq 0$.

(1) Is $(-1, -4)$ in R?

(2) Is $(-4, 0)$ in R?

(3) Is $(-1, 0)$ in R?

(4) Is $(0, 3)$ in R?

(5) Is $(-4, 3)$ in R?

(6) Is R transitive? If not, why?

ANSWER:

(1) Yes.
(2) Yes.
(3) Yes.
(4) Yes.
(5) No.
(6) No; for example, (-4, 0) is in R and (0, 3) is in R, but (-4, 3) is not in R.

- -

If you had difficulty with the preceding item it is possible that you have forgotten that in order for a relation R to be transitive, the condition that whenever (x, y) and (y, z) are in R then (x, z) is in R must hold in all cases. In the preceding example there are lots of cases where this is true; e.g., (-1, -4) and (-4, 0) are in R and (-1, 0) is also in R. However, if this condition fails in any one case then R is not transitive. Another way of saying this is that transitivity is a property of the whole relation R and not of any particular three ordered pairs in R.

Let S be the set of natural numbers {1, 2, 3, ...} and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and $x \cdot y$ is an even natural number. Some of the ordered pairs in R would be:

{(1, 2), (2, 4), (1, 4), (4, 6), (1, 6), (4, 3), ...}

Is R transitive? If not, why?

- -

ANSWER:

No; for example, (1, 4) and (4, 3) are in R, but (1, 3) is not.

- -

Let S be the set of all lines in a plane, and R be the set of all ordered pairs (ℓ, m) such that ℓ is in S, m is in S, and $\ell \perp m$. Is R a transitive relation?

ANSWER:

No.

In the example above, is R a symmetric relation?

ANSWER:

Yes.

Let S be the set of all real numbers, and $x \, R \, y$ if and only if $x < y$.

Is R a transitive relation?

ANSWER:

Yes.

Is R a symmetric relation?

ANSWER:

No.

DEFINITION 14.4: A relation R in a set S is said to be *antisymmetric* if and only if it satisfies the condition: whenever (a, b) is in R, then (b, a) is *not* in R (or, if $a \, R \, b$, then not $b \, R \, a$).

If R is antisymmetric, then $a \, R \, a$ is not true for any element a, that is, (a, a) is not in R for any element a. For if we take $a = b$ in Definition 14.4 we have the statement: if (a, a) is in R then (a, a) is not in R. Clearly (a, a) cannot be in R.

If R is not symmetric, is it antisymmetric?

ANSWER:

Not necessarily. (See the next items.)

Let S be the set of all real numbers and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and $x \geq y$.

Is R antisymmetric? If not, why?

ANSWER:

No; (x, x) is in R for each x in S. (Note that if R is antisymmetric it must be true that if (a, b) is in R, then (b, a) is not in R for every ordered pair (a, b). Antisymmetry is a property of R and not of a particular pair (a, b) in R.)

Is R symmetric? If not, why?

ANSWER:

No; for example $(4, 3)$ is in R, but $(3, 4)$ is not in R.

Thus the above relation is neither symmetric nor antisymmetric.

Let S be the set of all real numbers and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and $x > y$.

Is R symmetric?

Is R antisymmetric?

- -

ANSWER:

No.

Yes.

- -

Let S be the set of all human beings, and let R be the set of all ordered pairs (a, b) of human beings such that a is the father of b.

Is R symmetric?

Is R antisymmetric?

- -

ANSWER:

No.

Yes.

- -

Let $S = \{a, b\}$.

List all the non-empty subsets of S.

- -

ANSWER:

$\{a\}$, $\{b\}$, $\{a, b\}$.

- -

Let $S = \{a, b\}$ and R be the set of all ordered pairs (A, S) of sets such that A is a non-empty subset of S. Thus the elements of R are ordered pairs whose first and second members are sets.

List the ordered pairs of sets that belong to R.

- -

ANSWER:

R = {({a}, {a, b}), ({b}, {a, b}), ({a, b}, {a, b})}. R is a set with three elements. Each of these elements is an ordered pair of sets; e.g., ({b}, {a, b}).

Is R symmetric? If not, why?

ANSWER:

No; for example, ({a}, {a, b}) is in R, but ({a, b}, {a}) is not in R.

Is R antisymmetric? If not, why?

ANSWER:

No; the ordered pair ({a, b}, {a, b}) is in R.

DEFINITION 14.5: If S is any non-empty set, we define a relation in S to be an equivalence relation in S if and only if it is reflexive in S, symmetric, and transitive.

It should be noted that the reflexive property depends on the given set S, and a relation R is reflexive in S if and only if the ordered pair (a, a) is in R for every a in S, whereas the symmetric and transitive properties depend only on the elements in R.

Let S be the set of all plane triangles, and R be the set of all ordered pairs (x, y) such that x is in S, y is in S, and the triangle x is similar to the triangle y. Is R an equivalence relation? If not, why?

ANSWER:

Yes; R is reflexive, symmetric, and transitive.

Let $S = \{a, b\ c\}$

and $R = \{(a, a), (a, b), (b, a), (b, b)\}$

Is R an equivalence relation in S? If not, why?

ANSWER:

No; R is not reflexive in S since c is in S but (c, c) is not in R.

In the set of real numbers, the sentence "If $x - 2y = 7$, then $7 = x - 2y$" is an illustration of the ____ property of the relation "is equal to".

ANSWER:

symmetric

In the set of real numbers, the sentence "If $3x = a$ and $a = 4y$, then $3x = 4y$" is an illustration of the ____ property of the relation "is equal to".

ANSWER:

transitive

DEFINITION 14.6: A relation in a set S is an order relation if and only if it is antisymmetric and transitive.

Let S be the set of positive integers and R be the set of all ordered pairs (a, b) of positive integers such that a is a divisor of b and $a \neq b$.

Is R antisymmetric? If not, why?

- -

ANSWER:

Yes.

- -

Is R transitive? If not, why?

- -

ANSWER:

Yes.

- -

Is R an order relation?

- -

ANSWER:

Yes.

- -

Let $T = \{a, b, c\}$ and let S be the set of all non-empty subsets of T. List the elements of S.

- -

ANSWER:

$S = \left\{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\right\}$

- -

Let R be the relation in S (above) such that the ordered pair (S_1, S_2) is in R if and only if S_1 and S_2 are in S, $S_1 \subset S_2$, and $S_1 \neq S_2$.

Is $\mathcal{R}$ an order relation? If not, why?

ANSWER:

Yes.

Would $\mathcal{R}$ still be an order relation if we removed the restriction $S_1 \neq S_2$ in the example above? If not, why?

ANSWER:

No; $\mathcal{R}$ would no longer be antisymmetric.

Let S be the set of all real numbers and let $\mathcal{R}$ be the set of all ordered pairs (x, y) of real numbers such that $x < y$.

Is $\mathcal{R}$ an order relation? If not, why?

ANSWER:

Yes.

Is $\mathcal{R}$ an equivalence relation? If not, why?

ANSWER:

No; $\mathcal{R}$ is not symmetric (or reflexive in S).

Can an order relation be an equivalence relation? If not, why?

ANSWER:

No; an order relation can neither be symmetric nor reflexive in S, hence cannot be an equivalence relation.

To decide if R is transitive, you must check that for every ____.

ANSWER:

(x, y) and (y, z) in R, (x, z) is in R.

To decide if R is antisymmetric, you must check that for every ___.

ANSWER:

(x, y) in R, (y, x) is *not* in R.

To decide if R is an *equivalence relation* in S, you must check to see if R is ____.

ANSWER:

reflexive *in S*, symmetric, and transitive.

To decide if R is an *order relation*, you must check to see if R is ____ and ____.

ANSWER:

antisymmetric
transitive

In Unit IV we assumed that there was an "order relation" for the set of real numbers. We denoted this relation by "<". We assumed four postulates for this relation, 01, 02, 03, 04.

01 If a and b are real numbers then one, and only one, of the following is true, $a < b$, $a = b$, $b < a$.

From 01 we can conclude that the order relation for the set of real numbers is ____ (reflexive, symmetric, transitive, antisymmetric).

- -

ANSWER:

antisymmetric

- -

02 If a, b, c are real numbers such that $a < b$ and $b < c$ then $a < c$.

Postulate 02 tells us that the order relation for the set of real numbers is ___.

- -

ANSWER:

transitive.

- -

We see that the order relation for the set of real numbers satisfies the condition of Definition 14.6.

EQUIVALENCE RELATIONS AND EQUIVALENCE CLASSES

A relation in a set S is called an equivalence relation in S if what three properties are satisfied?

- -

ANSWER:

If the relation is reflexive in S, symmetric, and transitive. (Be sure to include "reflexive in S.")

- -

If R is a relation in a set S, then R is reflexive in S provided that ____.

- -

ANSWER:

(a, a) is in R for every element a in S.

- -

A relation R is symmetric provided that ____.

- -

ANSWER:

if (a, b) is an ordered pair in R then (b, a) is also in R.

- -

Let R be the relation in the set I of integers consisting of all ordered pairs (m, n) such that m and n have the same remainder when divided by two. Is R an equivalence relation in I? Test and explain each of the three required properties.

- -

ANSWER:

Yes. The pair (m, m) is in R for every m in I, so R is reflexive in I. If (m, n) is in R, then m and n have the same remainder when divided by two; hence (n, m) is in R, and we conclude that R is symmetric. The relation is transitive, because if (m, n) and (n, p) are in R, then m and p have the same remainder when divided by two, i.e., (m, p) is in R.

- -

Note that the above relation R partitions the set of integers into two nonoverlapping subsets. What are the names usually given to these two subsets?

- -

ANSWER:

The set O of odd integers (corresponding to remainder 1) and the set E of even integers (corresponding to remainder 0).

- -

DEFINITION 14.7: A set {A, B, C, ...} of subsets of a set S is a partition of S if the following conditions are satisfied:

(1) Each element of the set S is an element of one of the sets A, B, C, ...;

(2) No element of S is an element of two or more of the sets A, B, C, ... Thus each integer is in either the set O of odd integers or the set E of even integers and no integer is in both O and E. So $\{O, E\}$ is a partition of the set of integers.

Let S be the set of real numbers, A the set of positive real numbers, B the set of negative real numbers, and C = {0}. Is {A, B, C} a partition of S? If not, why not?

- -

ANSWER:

Yes, it is a partition of S.

- -

Let S be the set of integers, A the set of prime integers, and B the set of composite integers. Is {A, B} a partition of S? If not, why not?

- -

ANSWER:

No. The integers 0, 1, and -1 are not in A or in B.

Let S be a set and let {A, B, C, ...} be a partition of S. Define a relation R in S such that if a and b are elements, then (a, b) is in R provided that a and b are in the same set of the partition, i.e., if a and b are both in A, or are both in B, or are both in C, etc. We say that R is the relation in S determined by the partition {A, B, C, ...}.

For example, if S = {1, 2, 3, 4, 5, 6}, A = {1, 3, 4}, B = {2, 6}, and C = {5}, R contains 14 ordered pairs. List them.

ANSWER:
R = {(1, 1), (1, 3), (1, 4), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), (4, 4), (2, 2), (2, 6), (6, 2), (6, 6), (5, 5)}.

Let S be a set, let {A, B, C, ...} be a partition of S, and let R be the relation in S determined by the partition. Show that R is an equivalence relation. Test and explain each of the three required properties.

ANSWER:
If a is in S, then (a, a) is in R, because a is in some set of the partition and obviously a is in the same set of the partition as a. So R is reflexive in S. If (a, b) is in R, then a and b are in the same set of the partition; hence (b, a) is in R. Therefore R is symmetric. If (a, b) and (b, c) are in R, then a and b are in the same set of the partition and b and c are in the same set of the partition. Since each element of S lies in exactly one set of the partition, a and c must lie in the same set (the one containing b). Hence; (a, c) is in R. Therefore R is transitive.

We see that every partition of a set S determines an equivalence relation in the set S.

Suppose every set in a partition of S has exactly one element. What is the equivalence relation in S determined by the partition?

- -

ANSWER:

The equality relation in S. If a and b are in the same set of the partition then a = b, since each set contains only one element.

- -

If R is an equivalence relation in a set S then R determines a partition of S. If a and b are elements of S then a and b are in the same set of the partition if and only if (a, b) is in the relation R. More formally, for each element a in S we define a subset A_a of S to consist of all elements b such that (a, b) is in R.

An element a will be in the subset A_a because the equivalence relation R is ____.

- -

ANSWER:

reflexive in S.

- -

The symmetric property of R tells us that if b is in A_a, then ____.

- -

ANSWER:

a is in A_b.

- -

Using the transitive property of R we can show that if the sets A_a and A_b have any element in common then they are the same set. For suppose an element c is in both A_a and A_b. Then the ordered pairs ____ and ____ are in R.

- -

ANSWER:

(a, c) and (b, c)

- -

By the symmetric property (c, b) is in R, then by the transitive property ____ is in R.

- -

ANSWER:

(a, b)

- -

To show that $A_b \subset A_a$, we assume that d is an arbitrary element of A_b and prove that d is also an element of A_a. The ordered pair (b, d) is an element of R because ____.

- -

ANSWER:

d is in A_b.

- -

We have shown that (a, b) is in R. By the transitive property of R we conclude that ____.

- -

ANSWER:

(a, d) is in R.

- -

Hence d is in A_a. Therefore $A_b \subset A_a$. Similarly we can show that $A_a \subset A_b$. Together these imply that $A_a = A_b$. We conclude that no element of S is in two different subsets of the form A_a. Since every element of S is in exactly one of these sets, we have a partition of S.

DEFINITION 14.8: Each of the subsets in the partition determined by an equivalence relation is called an equivalence class of the relation.

Does the phrase "has the same remainder when divided by 3" describe an equivalence relation in the set of integers?

- -

ANSWER:

Yes.

- -

How many equivalence classes are determined by the above equivalence relation?

- -

ANSWER:

Three.

- -

List four elements in the equivalence class A containing 2.

- -

ANSWER:

$A = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$.

- -

List four elements in each of the other two classes.

- -

ANSWER:

B = {..., -6, -3, 0, 3, 6, 9, ...}

C = {..., -5, -2, 1, 4, 7, 10, ...}

- -

There is a special notation which is used to indicate that an ordered pair (a, b) is in the relation just described. It is "$a \equiv b \pmod{3}$", which is read "a is congruent to b modulo 3". For example, since 10 and -5 each have remainder 1 when divided by 3, the ordered pair (10, -5) is in the relation and we would write ____.

- -

ANSWER:

$10 \equiv -5 \pmod{3}$

- -

We use similar notation when some other positive integer is used in place of 3. For example, replacing 3 by 7, since 10 and 31 each have remainder 3 when divided by 7 we would write ____.

- -

ANSWER:

$10 \equiv 31 \pmod{7}$

- -

We have $16 \equiv -2 \pmod{6}$ because ____.

- -

ANSWER:

16 and -2 have the same remainder (4) when divided by 6.

- -

In general, if m is a positive integer greater than 1, then "$a \equiv b \pmod{m}$" means that the integers ____ and ____ have the same remainder when divided by ____.

- -

ANSWER:

a, b, m.

If m is any integer greater than 1, then congruence modulo m is an equivalence relation on the set of integers.

In the examples that we have given above we note the following:

(a) $10 \equiv -5 \pmod{3}$ and $10 - (-5)$, which is divisible by 3.

(b) $10 \equiv 31 \pmod{7}$ and $10 - 31 = -21$, which is divisible by 7.

(c) $16 \equiv -2 \pmod{6}$ and $16 - (-2) = 18$, which is divisible by 6.

Each of these examples illustrates the following theorem:

THEOREM 14.1a: If a and b are integers, m is a positive integer greater than 1, and if $a \equiv b \pmod{m}$, then $a - b$ is divisible by m.

Prove Theorem 14.1a.

ANSWER:

If $a \equiv b \pmod{m}$ then a and b have the same remainder when divided by m; i.e., $a = mq + r$ and $b = mp + r$. Then $a - b = mq - mp = (q - p)m$.

State the converse of Theorem 14.1a. Label it Theorem 14.1b.

ANSWER:

THEOREM 14.1b: If a and b are integers and m is a positive integer greater than 1, and if $a - b$ is divisible by m, then $a \equiv b \pmod{m}$.

Prove Theorem 14.1b.

If you feel that you have given a complete proof, go to the $\boxed{\dagger\dagger}$ below. If not, go to the next item below.

Suppose $a = mq + r$, $0 \leq r < m$, and $b = mp + s$, $0 \leq s < m$. We have to show that ____.

ANSWER:

$r = s$.

This may be done by showing that $r - s$ is divisible by m. Go back to your proof. Make additions or corrections before proceeding. Then go to the next item.

$\boxed{\dagger\dagger}$ ANSWER:

PROOF: Suppose $a = mq + r$, $0 \leq r < m$, and $b = mp + s$, $0 \leq s < m$. $a - b = m(q - p) + r - s$. So $r - s = a - b - m(q - p)$. If $a - b$ is divisible by m then so is $r - s$. Since r and s are non-negative integers less than m, we have $-m < r - s < m$. Therefore $r - s = 0$, and $r = s$. It follows that $a \equiv b \pmod{m}$.

THEOREM 14.2a: If a, b, and c are integers, m is a positive integer greater than 1, and if $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$.

Prove Theorem 14.2a.

ANSWER:

PROOF: If $a \equiv b \pmod{m}$, then $a - b$ is divisible by m, by Theorem 14.1a. Then, since $(a + c) - (b + c) = a + c - b - c = a - b$, $(a + c) - (b + c)$ is divisible by m. By Theorem 14.1b, $a + c \equiv b + c \pmod{m}$.

Write the converse of Theorem 14.2a.

ANSWER:

If a, b, and c are integers, m is a positive integer greater than 1, and if $a + c \equiv b + c \pmod{m}$, then $a \equiv b \pmod{m}$.

If the above statement is true, prove it. If it is not true, give an example to show it is false.

ANSWER:

The statement is true.

PROOF: Since $a + c \equiv b + c \pmod{m}$, we have $a + c - (b + c)$ is divisible by m. $a + c - (b + c) = a + c - b - c = a - b$. Therefore $a - b$ is divisible by m and $a \equiv b \pmod{m}$. We have used Theorems 14.1a and 14.1b.

Alternate Proof:

$a + c \equiv b + c \pmod{m}$	Hypothesis
$a + c + (-c) \equiv b + c + (-c) \pmod{m}$	Theorem 14.2a
$a \equiv b \pmod{m}$	

We will call the converse of Theorem 14.2a Theorem 14.2b.

THEOREM 14.2b: If a, b, and c are integers, m is a positive integer greater than 1, and if $a + c \equiv b + c \pmod{m}$, then $a \equiv b \pmod{m}$.

Prove the following theorem:

THEOREM 14.3: If a, b, and c are integers, if m is a positive integer greater than 1, and if $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$.

ANSWER:

PROOF: $a \equiv b \pmod{m} \Longleftrightarrow a - b$ is divisible by m. Therefore $(a - b)c$ is divisible by m. $(a - b)c = ac - bc$, so $ac \equiv bc \pmod{m}$. (Theorems 14.1a and 14.1b).

Write the converse of Theorem 14.3.

ANSWER:

If a, b, c are integers, m is a positive integer greater than 1, and if $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

If the above statement is true, prove it. If it is not true, disprove it.

ANSWER:

The converse of Theorem 14.3 is not true. For example, $14 \equiv 2 \pmod{12}$ but $7 \not\equiv 1 \pmod{12}$.

We have shown that congruence has properties corresponding to the following properties of equality of numbers.

(1) If $a = b$, then $a + c = b + c$.
(2) If $a + c = b + c$, then $a = c$.
(3) If $a = b$, then $ac = bc$.

We have shown that the cancellation property for multiplication is not always true, for congruences, by demonstrating that $14 \equiv 2 \pmod{12}$ does not imply that $7 \equiv 1 \pmod{12}$. However, $14 \equiv 2 \pmod{3}$ and $7 \equiv 1 \pmod{3}$. In multiplication in congruences we can cancel in some cases.

Let us try to prove the cancellation property for multiplication and see where we get stuck.

If $ac \equiv bc \pmod{m}$, then m is a divisor of $ac - bc$. Thus m is a divisor of $(a - b)c$. What additional condition can we place on m and c in order to be able to conclude that if m is a divisor of $(a - b)c$, then m is a divisor of $a - b$?

- -

ANSWER:
If m and c are relatively prime, we have the required conclusion.

- -

THEOREM 14.4: If a, b, and c are integers, m is a positive integer greater than 1, and if m and c are relatively prime and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

If a and b are integers and $a - b = 12$, for what choices of m (m to be an integer greater than 1) do we have $a \equiv b \pmod{m}$?

- -

ANSWER:
$m = 2, 3, 4, 6, 12$.

- -

What is the smallest positive value for b in $75 \equiv b \pmod{9}$?

ANSWER:

3.

What is the largest negative value for b in $93 \equiv b \pmod{7}$?

ANSWER:

-5.

$17 \equiv 4 \pmod{13}$. For what integer values of c will $17 + c \equiv 4 + c \pmod{13}$ hold?

ANSWER:

All integer values of c.

What two equivalence classes are formed by congruence modulo 2?

ANSWER:

Even integers and odd integers.

Let us denote the equivalence class of even integers by α and the equivalence class of odd integers by β. It is possible to set up an arithmetic for these equivalence classes; e.g., $\alpha + \alpha = \alpha$, the sum of two even numbers is even. Using your experience with the sums and products of odd and even integers, make the following addition and multiplication tables for congruence modulo 2.

+	α	β
α	α	
β		

·	α	β
α		
β		

- -

ANSWER:

+	α	β
α	α	β
β	β	α

·	α	β
α	α	α
β	α	β

- -

Now form the addition and multiplication tables for arithmetic modulo 2; i.e., for the elements 0 and 1.

- -

ANSWER:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

- -

Compare the addition and multiplication tables for arithmetic modulo 2 with the corresponding tables for the equivalence classes modulo 2. What name do we give to the relationship between the two arithmetics?

- -

ANSWER:

Isomorphism.

- -

Congruence modulo 3 is an equivalence relation in the set of integers. There are three equivalence classes, given as follows:

$\alpha = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$\beta = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

$\gamma = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$

We can form an arithmetic from the classes $\{\alpha, \beta, \gamma\}$. If we add any two elements of α we get an element of α. Hence we define $\alpha + \alpha = \alpha$. If we add any element of α to any element of β we get an element of ____..

ANSWER:

β.

Therefore we define $\alpha + \beta = \beta$. Similarly, if we multiply any element of β by any element of γ we get an element of ____.

ANSWER:

γ.

Therefore we define $\beta \cdot \gamma = \gamma$

Proceeding by analogy, complete the following addition and multiplication tables:

+	α	β	γ
α	α	β	
β			
γ			

$\cdot$	α	β	γ
α			
β			γ
γ			

ANSWER:

+	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	β

•	α	β	γ
α	α	α	α
β	α	β	γ
γ	α	γ	β

Recall that the addition and multiplication tables for I/3 = {0, 1, 2} are as follows:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

A comparison of the two pairs of tables shows that the arithmetic of the classes {α, β, γ} is isomorphic to the arithmetic I/3. An extension of this would show that if n is any positive integer greater than 1, then the arithmetic I/n is isomorphic to the arithmetic of equivalence classes of congruence modulo n.

GROUPS

In an earlier unit (Unit II) we have introduced the notion of a group.

A non-empty set G on which there is defined a closed binary operation "o" is called a group with respect to the operation "o" if the following properties are satisfied:

i. ____.

ii. ____.

iii. ____.

ANSWER:

i. If a, b, c are in G, then $(a \text{ o } b) \text{ o } c = a \text{ o } (b \text{ o } c)$. (associative property)

ii. There exists an element e of G such that $e \text{ o } a = a \text{ o } e = a$ for all a in G. (identity property)

iii. If a is in G, there exists an element x in G such that $a \text{ o } x = x \text{ o } a = e$. (inverse property)

We denote x in iii by a^{-1}.

If the operation "o" also satisfies the commutative property, the group is called a ____.

ANSWER:

commutative group.

Commutative groups are sometimes called Abelian groups in honor of a famous Norwegian mathematician Niels Abel (1802-1829).

Examples of commutative groups abound in the real and complex number systems; i.e., there are many subsets of these number systems which form groups with respect to either the addition operation or the multiplication operation. In each of the following a subset of the real or complex number system is given together with one of the operations, addition and multiplication. For each, determine if it is a group and, if not, explain why.

(a) the set of positive integers -- addition.

(b) the set of positive integers -- multiplication.

(c) the set of positive rational numbers -- multiplication.

(d) the set of complex numbers of form $a \cdot i$, for all real numbers a -- addition.

(e) the set of complex numbers $\{1, -1, i, -i\}$ -- multiplication.

- -

ANSWER:

(c), (d), and (e) are groups. In example (a) the conditions ii and iii of the definition of group are not satisfied. In example (b) the condition iii is not satisfied.

- -

If n is a positive integer greater than 1, then the arithmetic I/n is a group under the addition operation. If n is a prime positive integer then the arithmetic I/n^* (non-zero elements of I/n) is a group under the multiplication operation.

Another source of examples of groups are the sets of functions from a set X onto X. Recall that if f is a function from X onto X, then X is both the ____ and the ____ of f.

- -

ANSWER:

domain

range

- -

Also recall that if f and g are functions from X onto X, then the composite of f with g is the function $f \circ g$ defined as follows: if x is in X and if $x \xrightarrow{g} g(x)$ and $g(x) \xrightarrow{f} f(g(x))$ then $x \xrightarrow{f \circ g}$ ____. In other notation, $(f \circ g)(x) =$ ____.

- -

ANSWER:

$f(g(x))$.

$f(g(x))$.

- -

The operation "o", called "composition", assigns each ordered pair of functions from X onto X to a function. Hence it is a binary operation on the set of functions from X onto X.

In order to be able to test the properties of this operation we need to recall the definition of equality of functions. If f and g are functions with domain X, then f = g if and only if f(x) = g(x) for every x in X.

Is composition an associative operation? We may answer this question by examining the following statements.

If f, g, and h are functions from X onto X, then by definition ((f o g) o h)(x) = (f o g)(h(x)) = f(g(h((x))); and (f o(g o h)) (x) = ____ = ____.

- -

ANSWER:

f((g o h)(x)) = f(g(h(x))).

- -

Thus ((f o g) o h)(x) = (f o (g o h))(x) for every x in X. By the definition of equality of functions ____ = ____.

- -

ANSWER:

(f o g) o h = f o (g o h).

- -

We will now see that if f and g are functions from X onto X then f o g is an onto function. To prove that f o g is onto we must show that if y is any element of X, then ____.

- -

ANSWER:

there is an element x in X such that $f \circ g(x) = y$ (or $x \xrightarrow{fog} y$).

It is helpful to consider the problem with the following notation: if x is an element of X and $g(x) = z$ and if $f(z) = y$, then

$$\begin{tikzcd} x \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & z \arrow[r, "f"] & y. \end{tikzcd}$$

If f and g are functions from X onto X, and y is a given element of X, explain why there must be elements x and z in X as indicated in the above diagram.

ANSWER:

Because f is onto, there must be an element z in X such that $z \xrightarrow{f} y$. Then, because g is onto, there must be an element x in X such that $x \xrightarrow{g} z$. Then $x \xrightarrow{fog} y$.

This proves that $f \circ g$ is onto.

How is the identity function I on X defined?

ANSWER:

$I(x) = x$, for each element x in X.

Is the identity function a function from X onto X?

ANSWER:

Yes.

Find $(I \circ f)(x)$ and $(f \circ I)(x)$, for x an element of X and f a function from X onto X.

ANSWER:

$(I \circ f)(x) = I(f(x)) = f(x)$ and $(f \circ I)(x) = f(I(x)) = f(x)$.

Therefore $I \circ f = f \circ I = f$, for each function f from X onto X.

Now let G be the set of functions from X onto X which are also reversible. Recall that f is reversible if ____ is a function.

ANSWER:

f^{-1}

If f is a reversible function from X onto Y, what are the domain and range of f^{-1}?

ANSWER:

The domain of f^{-1} is Y.

The range of f^{-1} is X.

If f is a reversible function from X onto X, then f^{-1} is a reversible function from X onto X, and $f \circ f^{-1} = f^{-1} \circ f =$ ____.

ANSWER:

I.

A function f from X onto X is reversible if f does not contain two ordered pairs with the same second member and different first members. Hence if x_1 and x_2 are elements of X and $x_1 \neq x_2$, and if $x_1 \xrightarrow{f} y_1$, $x_2 \xrightarrow{f} y_2$ then ____.

ANSWER:

$y_1 \neq y_2$.

Assume that f and g are reversible functions from X onto X and that x_1 and x_2 are elements of X such that $x_1 \neq x_2$. Suppose

$$\begin{tikzcd} x_1 \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & z_1 \arrow[r, "f"] & y_1 \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} x_2 \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & z_2 \arrow[r, "f"] & y_2 \end{tikzcd}$$

To show that $f \circ g$ is reversible, we must show that $y_1 \neq y_2$. Why does $z_1 \neq z_2$?

ANSWER:

Because g is reversible. $x_1 \neq x_2$ and $x_1 \xrightarrow{g} z_1$, $x_2 \xrightarrow{g} z_2$, imply that $z_1 \neq z_2$.

Since f is reversible, $z_1 \neq z_2$, and $z_1 \xrightarrow{f} y_1$, $z_2 \xrightarrow{f} y_2$, it follows that $y_1 \neq y_2$. This proves that $f \circ g$ is reversible. We have shown that the operation "o" is closed on the set G of reversible functions from X onto X. Furthermore the identity function I is an identity element for the operation "o"; and if f is in G, then f^{-1} is in G and is an inverse of f with respect to the operation "o" (i.e., $f^{-1} \circ f = f \circ f^{-1} = I$). This proves that G is a ____.

ANSWER:

group.

We have proved the following theorem.

THEOREM 14.5: If X is a non-empty set and G is the set of reversible functions from X onto X, then G, together with the operation of composition of functions, is a group.

We now consider an example. Let X be the set $\{a, b, c\}$, and let G be the group of one-to-one, or reversible, functions from X onto X. One of the elements of G is the function f defined by

f: $a \xrightarrow{f} c$
$b \xrightarrow{f} a$
$c \xrightarrow{f} b$

List the remaining functions in this set. (There are 5 more.)

ANSWER:

$f_1 = I$: $a \xrightarrow{I} a$
$b \xrightarrow{I} b$
$c \xrightarrow{I} c$

f_2: $a \xrightarrow{f_2} a$
$b \xrightarrow{f_2} c$
$c \xrightarrow{f_2} b$

f_3: $a \xrightarrow{f_3} b$
$b \xrightarrow{f_3} a$
$c \xrightarrow{f_3} c$

f_4: $a \xrightarrow{f_4} c$
$b \xrightarrow{f_4} b$
$c \xrightarrow{f_4} a$

f_5: $a \xrightarrow{f_5} b$
$b \xrightarrow{f_5} c$
$c \xrightarrow{f_5} a$

Let us designate the given example f_6.

Using the notation given in the above answer, $f_2 \circ f_4 =$ ____.
(Remember f_4 is performed first.)

ANSWER:

$a \xrightarrow{f_4} c \xrightarrow{f_2} b$

$b \xrightarrow{f_4} b \xrightarrow{f_2} c$

$c \xrightarrow{f_4} a \xrightarrow{f_2} a$

$\therefore f_2 \circ f_4 = f_5$

The inverse of f_5 is ____.

ANSWER:

f_6, since $f_5 \circ f_6 = f_6 \circ f_5 = I$.

O	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

The complete group table for G is given above.

Is G a commutative group?

ANSWER:

No; e.g., $f_2 \circ f_4 = f_5$ and $f_4 \circ f_2 = f_6$, so $f_2 \circ f_4 \neq f_4 \circ f_2$.

OTHER PROPERTIES OF A GROUP

If F is a field, the set of elements in F form a commutative group under the operation of addition and the set of non-zero elements form a commutative group under the operation of multiplication. Many of the theorems that we have obtained for fields require in their proofs only properties of a group. The proofs which we have given can often be altered slightly to yield proofs of theorems about groups.

Assume that G is a group under an operation "o". We will denote the identity element of G by e and the inverse of an element a of G by a^{-1}.

In the following pages you will be asked to prove several theorems about G. Each of these theorems is related to theorems about fields. In each case you should try to identify the related field theorems. There will usually be two such, one concerning addition in a field and the other concerning multiplication in a field.

THEOREM 14.6: If a and b are elements of G such that $a \circ b = b$, then $a = e$.

One of the related field theorems is the following:

If a and b are elements of a field F such that $a + b = b$, then $a = 0$.

What is the other related field theorem?

- -

ANSWER:

If a and b are elements of a field F, $b \neq 0$, such that $a \cdot b = b$, then $a = e$.

- -

Prove Theorem 14.6.

ANSWER:

Suppose $a \circ b = b$

Then $(a \circ b) \circ b^{-1} = b \circ b^{-1}$

$a \circ (b \circ b^{-1}) = b \circ b^{-1}$ Associative property of "o"

$a \circ e = e$ Property of b^{-1}

$a = e$ Property of e

THEOREM 14.7: If a and b are elements of G and $a \circ b = e$, then $b = a^{-1}$, and $a = b^{-1}$.

State two field theorems which are related to Theorem 14.7.

ANSWER:

(1). If a and b are elements of a field F and $a + b = 0$, then $b = -a$.

(2). If a and b are elements of a field F and $ab = 1$, then $b = a^{-1}$.

Prove Theorem 14.7. You need not give reasons in your proof.

ANSWER:

Suppose $a \circ b = e$

Then $a^{-1} \circ (a \circ b) = a^{-1} \circ e$

$(a^{-1} \circ a) \circ b = a^{-1} \circ e$

$e \circ b = a^{-1} \circ e$

$b = a^{-1}$

The proof that $a = b^{-1}$ is similar.

THEOREM 14.8: If a, b, and c are in G and $a \circ b = a \circ c$, then $b = c$.

Prove Theorem 14.8. You need not give reasons.

ANSWER:

Suppose $a \circ b = a \circ c$

$$\begin{aligned} \text{Then } a^{-1} \circ (a \circ b) &= a^{-1} \circ (a \circ c) \\ (a^{-1} \circ a) \circ b &= (a^{-1} \circ a) \circ c \\ e \circ b &= e \circ c \\ b &= c \end{aligned}$$

THEOREM 14.9: If a and b are elements of G there exists a unique element x of G such that $a \circ x = b$ and a unique element y of G such that $y \circ a = b$.

Write x and y in terms of b and a^{-1}.

ANSWER:

$x = a^{-1} \circ b$, $y = b \circ a^{-1}$

Note that x and y may not be the same since we are not assuming that the operation in G is commutative.

Prove that if $x = a^{-1} \circ b$ and $y = b \circ a^{-1}$, then $a \circ x = b$ and $y \circ a = b$. You need not give reasons.

ANSWER:

$$\begin{aligned}
\text{If}\quad x &= a^{-1} \circ b, \text{ then} \\
a \circ x &= a \circ (a^{-1} \circ b) \\
&= (a \circ a^{-1}) \circ b \\
&= e \circ b \\
&= b
\end{aligned}$$

$$\begin{aligned}
\text{If}\quad y &= b \circ a^{-1}, \text{ then} \\
y \circ a &= (b \circ a^{-1}) \circ a \\
&= b \circ (a^{-1} \circ a) \\
&= b \circ e \\
&= b
\end{aligned}$$

Prove that x and y are unique by showing that if $a \circ x = b$ and $y \circ a = b$, then $x = a^{-1} \circ b$ and $y = b \circ a^{-1}$. You need not give reasons.

ANSWER:

Suppose $a \circ x = b$ and $y \circ a = b$.

$$\begin{aligned}
\text{Then}\quad a^{-1} \circ (a \circ x) &= a^{-1} \circ b \\
(a^{-1} \circ a) \circ x &= a^{-1} \circ b \\
e \circ x &= a^{-1} \circ b \\
x &= a^{-1} \circ b
\end{aligned}$$

$$\begin{aligned}
\text{and}\quad (y \circ a) \circ a^{-1} &= b \circ a^{-1} \\
y \circ (a \circ a^{-1}) &= b \circ a^{-1} \\
y \circ e &= b \circ a^{-1} \\
y &= b \circ a^{-1}
\end{aligned}$$

Hence the only possibility for x is $a^{-1} \circ b$ and for y is $b \circ a^{-1}$.

THEOREM 14.10: If a and b are elements of G, then $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Note that if G is not commutative then in general $b^{-1} \circ a^{-1}$ is not the same as $a^{-1} \circ b^{-1}$.

Prove Theorem 14.10.

ANSWER:

$$\begin{aligned}(b^{-1} \circ a^{-1}) \circ (a \circ b) &= b^{-1} \circ (a^{-1} \circ (a \circ b)) \\ &= b^{-1} \circ ((a^{-1} \circ a) \circ b) \\ &= b^{-1} \circ (e \circ b) \\ &= b^{-1} \circ b \\ &= e\end{aligned}$$

By Theorem 14.7, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

REVIEW ITEMS

How many equivalence classes are determined by the equivalence relation, congruence modulo 17?

ANSWER:

17

List four elements of the equivalence class of congruence modulo 17 which contain the integer 10.

ANSWER:

{..., -41, -24, -7, 10, 27, 44, ...}

Let S = {1, 2, 3, 4, 5} and let A = {1, 4, 5}, B = {2, 3}. List all the ordered pairs in the equivalence relation on S determined by the partition {A, B}.

ANSWER:

(1, 1), (1, 4), (1, 5), (4, 1), (4, 4), (4, 5), (5, 1), (5, 4), (5, 5), (2, 2), (2, 3), (3, 2), (3, 3).

Suppose a is an integer and $a^4 \equiv 2 \pmod{11}$. Find a positive integer b less than 11 such that $a^{20} \equiv b \pmod{11}$.

ANSWER:

b = 10. Solution: $a^4 \equiv 2 \pmod{11}$ implies $a^4 \cdot a^4 \equiv 2 \cdot a^4 \pmod{11}$, or $a^8 \equiv 2a^4 \pmod{11}$. But $a^4 \equiv 2 \pmod{11}$ also implies $2a^4 \equiv 2 \cdot 2 \pmod{11}$. Thus $a^8 \equiv 4 \pmod{11}$. Proceeding in this way we get $a^{12} \equiv 8 \pmod{11}$, $a^{16} \equiv 16 \pmod{11}$, $a^{20} \equiv 32 \pmod{11}$. But $32 \equiv 10 \pmod{11}$. Therefore $a^{20} \equiv 10 \pmod{11}$.

Prove: If a, b, c, d are integers, n is a positive integer greater than 1, and if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$. Give reasons. [Hint: Apply Theorem 14.2 twice.]

ANSWER:

$a \equiv b \pmod{n}$	Hypothesis
$a + c \equiv b + c \pmod{n}$	Theorem 14.2
$c \equiv d \pmod{n}$	Hypothesis
$b + c \equiv b + d \pmod{n}$	Theorem 14.2
$a + c \equiv b + d \pmod{n}$	Transitive property of congruence modulo n

---

Let $X = \{a, b\}$ and let G be the group of one-to-one functions from X onto X. Describe the functions in G and give the group table for G.

ANSWER:

$G = \{I, f\}$, where

$I: a \longrightarrow a$ $\quad$ $f: a \longrightarrow b$

$\quad\;\; b \longrightarrow b$ $\quad\quad\;\; b \longrightarrow a$

Table:

·	I	f
I	I	f
f	f	I

State two field theorems which are related to Theorem 14.8.

ANSWER:

(1) If a, b, and c are in F and $a + b = a + c$, then $b = c$.

(2) If a, b, and c are in F and $a \neq 0$, and if $a \cdot b = a \cdot c$, then $b = c$.

This programmed text is designed to increase understanding of some of the basic ideas of Algebra. Some general experience and manipulative skill with respect to high school algebra is presumed on the part of the student. Emphasis has been placed upon development of the logical structure. There is a rigorous development of the rules of algebra based upon precise definitions and clearly stated basic assumptions (or postulates). Major emphasis has been placed upon the real number system. Various mathematical systems which are different from the real number system but which share some of its properties are compared and contrasted with it. In this way the properties of real numbers should be made clearer.

In addition, a Summary Textbook for the programmed course is available. Its purpose is to provide the student with a complete, but condensed, summary and index of the content of the program for the purpose of reference and review.

Ancel C. Mewborn is an Associate Professor of Mathematics at the University of North Carolina at Chapel Hill. He received his A.B., M.A., and Ph.D. degrees from the University of North Carolina and has formerly taught at Yale University. Dr. Mewborn is a member of the American Mathematical Society and the Mathematical Association of America, and his field of special interest is algebra and the theory of rings.

Wells Hively II is an Associate Professor and chairman of the Department of Psychological Foundations of Education at the University of Minnesota. He received his Ph.D. from Harvard and taught there before going to the University of Minnesota in 1963. Dr. Hively is a member of American Education Research Association, American Psychological Association, the American Association for the Advancement of Science, and the National Council of Measurement in Education. He is a specialist in programmed instruction.

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts
Menlo Park, California · London · Don Mills, Ontario

649